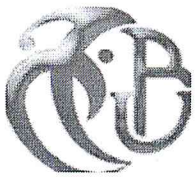
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSENGEMENT SUPERIEUR

Université SAAD DAHLEB-Blida



Faculté des Sciences

Département Informatique

En vu d'obtenir le diplôme de Master en Informatique

Thème:

Protection du Cloud Computing Contre les Attaques DoS.

Présenté par :

MANSOURI Zaineb

TELDJOUNE Zineb

Proposé par:

Mme OUKID

Encadré pas:

Mme Y.GHEBROUB

Soutenu le : 24/09/2013

Devant le Jury composé de :

Président : Dr. BENOUAR

Examinateurs : Melle GHENDOUZ

Examinateurs : Melle MENSER

Promotion: 2012-2013

DEDICACE

Nous dédions ce travail à mes très chers parents, qui m'ont éclairé le chemin de la vie par leurs grand soutien et leurs encouragements, qu'ils m'ont consentis durant mes études et qui ont toujours aimé me voire réussir, qu'ils trouvent ici toute ma gratitude et mes sentiments les plus respectueux.

A nos frères, A nos Sœurs, A nos grandes familles et tous qui ont

A nos amies et tous qui nous connaissons.

Et enfin à tous les étudiants de l'informatique.

Zineb & Zaineb

Remerciement

Au terme de ce travail nous tenons le remercier tout d'abord ALLAH qui nous donne la force et le courage et d'avoir facilité la réalisation de ce travail

Nous expriment notre grande respectes a nos parents et nos famille qui ont toujours encouragé.

La présentation de ce modeste ouvrage nous exprimons toute notre reconnaissance à notre Co-promotrice Mme GHEBGHOUB pour son soutien, ses conseils, et ses orientations qui nous ont été très utiles.

Nous adressons également nos remerciements à tous nos professeurs Qui nous ont enseigné durant notre cursus universitaire et à tous les professeurs de département d'informatique pour leurs efforts et leurs conseils.

Nous remercions vivement La directrice de la bibliothèque centrale et tous ses employeurs.

Nous remerciement vont également à tous Le personnel de l'université de Blida.

TABLES DES MATIERES

TABLES DES MATIERES

TABLES DES MATIERES

TABLES DES MATIERES

Listes des figures

Listes des figures

Résumé :

Le cloud computing est un des secteurs les plus dynamiques dans le monde, Le total des revenus pour 2016 est estimé à 210 billions de dollars. Un secteur avec une telle croissance est une cible attractive pour les criminels.

Le plus grand problème dans le cloud computing est que les clients n'ont pas confiance dans la sécurisation et la protection de leurs données. Il existe diverses attaques externes, mais on s'intéresse dans cette étude des attaques DoS (denial of service),

Une possibilité pour se protéger est l'implémentation d'un firewall qui permet de filtrer les paquets entrants et sortants afin de prévenir toutes attaques de l'extérieur. Ils se basent sur un fonctionnement séquentiel et un ensemble de règles pour autoriser seulement les connexions légitimes, pour perpétrer leurs attaques. De plus, les firewalls ne peuvent pas efficacement différencier les connexions légitimes et illégitimes. Par contre ils peuvent se révéler très efficace pour contre un attaquant. En se basant sur les informations fournit par des équipements de détections, on peut appliquer des règles très précises qui bloqueront uniquement les connexions malfaisantes, en se basant sur le protocole IP ou le port.

Introduction générale

Le **Cloud Computing** est une nouvelle manière de fournir et d'utiliser les aptitudes des systèmes informatiques basée sur les *nuages* (*Cloud* en anglais). Un nuage est un parc de machines, d'équipement de réseau et de logiciels maintenu par un fournisseur, que les consommateurs peuvent utiliser en libre-service via Internet. Les caractéristiques techniques du nuage ne sont pas connues du consommateur et les services sont payés à l'usage. Selon la définition du *National Institute of Standards and Technologie* (NIST), le *Cloud Computing* est l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées .

Aujourd'hui, il existe des modèles de Cloud Computing publics et privés. Les modèles publics, accessibles à quiconque dispose d'un accès Internet, recouvrent plusieurs types de nuages : les nuages SaaS (Software as a Service – logiciel en tant que service), comme IBM LotusLive ; les nuages PaaS (Platform as a Service– plateforme en tant que service), comme Amazon Web Services ; et les nuages SDPaaS (Security and Data Protection as a Service – sécurité et protection des données en tant que service), comme IBM Security Event and Log Management Services.

Grâce à la virtualisation, améliorez l'efficacité et la disponibilité de vos ressources et applications informatiques. Commencez par abandonner l'ancien modèle « un serveur, une application » et exécutez plusieurs machines virtuelles sur chaque machine physique. Allégez la tâche de vos administrateurs informatiques, qui passent plus de temps à gérer les serveurs qu'à innover. Dans un Datacenter non virtualisée, près de 70 % d'un budget informatique type sont consacrés à la simple maintenance de l'infrastructure existante, ce qui laisse peu pour l'innovation.

La **sécurité du Cloud** (*Cloud Security* en anglais) est un sous domaine du Cloud Computing (Informatique dans les nuages) en relation avec la sécurité informatique. Elle implique des concepts tels que la sécurité des réseaux, du matériel et les stratégies de contrôle déployées afin de protéger les données, les applications et l'infrastructure associée au Cloud Computing. Un aspect important du Cloud est la notion d'interconnexion avec divers matériels qui rend difficile et nécessaire la sécurisation de ces environnements.

Introduction générale

Un problème de sécurité dans une plateforme sur le Cloud peut engendrer une perte économique mais également une mauvaise réputation si toutefois cette plateforme est orientée grand public. Les problèmes de sécurité du Cloud sont la cause du retard de l'adoption massive de cette nouvelle solution.

Le plus grand problème dans le Cloud Computing est que les clients n'ont pas confiance dans la sécurisation et la protection de leurs données. Différents types de menaces existent. Il faut distinguer les attaques actives et passives et les attaques internes et externes. La détection des attaques passives est très difficile, car l'attaquant n'intervient pas directement dans le système d'information. Pendant une attaque active, l'attaquant agit directement dans le système par exemple en modifiant les informations, mais ces attaques laissent des traces qui peuvent aider à identifier le criminel.

Parmi ces divers problèmes de sécurité nous nous intéressons d'un type d'attaque qui s'appelle l'attaque Doss (denial of service en anglais ou DoS) sont des attaques qui visent à rendre une machine ou un réseau indisponible durant une certaine période. En apparence une telle attaque peut sembler inoffensive si elle vise un réseau ou un ordinateur particulier, mais elle peut s'avérer redoutable lorsqu'elle vise un serveur ou des ressources matérielles appartenant à une grande société dépendante de son infrastructure réseau. Ce genre d'attaque est très répandue sur les réseaux car elle est assez simple à mettre en œuvre mais peut néanmoins avoir des conséquences désastreuses. De plus la détection et la prévention de ces attaques sont très difficiles car elles peuvent prendre des formes très variées, quasiment tous les systèmes informatiques sont vulnérables et même des équipements coûtant des milliers de dollar ne peuvent parfois rien faire contre de telles attaques.

Problèmatique :

La disponibilité de l'accès à un service cloud est un aspect très important dans les systèmes d'information aujourd'hui spécialement pour le cloud computing.

Notre problématique est comment protéger la disponibilité des services de cloud en éliminent les causes de cette menaces plus précisement les attaques DoS de type SynFlood qui s'applique dans le cadre du protocole TCP et consiste à envoyer une succession de requêtes SYN vers la cible

Objectif :

Afin de trouver une solution pour ce type d'attaque nous traçons les objectifs suivants :

- Réalisation d'une architecture de cloud qui repose sur la virtualisation c'est-à-dire la création d'un cluster qui est un regroupement de machines sont appelées des « nœud ».
- Protection de notre réseau contre les attaques DoS.

Introduction :

Les couts informatiques (humain et financier) représentent une part importante de budget d'une entreprise. Une réponse à cette problématique est apparu le « Cloud Computing » par l'externalisation de l'informatique (logiciel et /ou matériel) et l'utilisation de la puissance de serveurs répartis dans le monde entier. Cette délocalisation est facilitée par internet.

Aujourd'hui, le « Cloud Computing » dispose de nombreux avantages semble être une solution séduisante, et l'imagination de la future (2016 in chaa allah) de ce nouveau mode de fonctionnement de l'entreprise.

1. Définition :

Le terme Cloud Computing ou <<informatique dans le nuage>> est une tapage émergée récemment dans la littérature informatique. La plupart des fournisseurs ont immédiatement introduit ce terme à tort et à travers dans leurs offres ce qui n'en simplifie pas la compréhension.

Le Cloud Computing est un « nouveau » modèle informatique qui consiste à proposer les services informatiques sous forme de services à la demande, accessibles de n'importe où, n'importe quand et par n'importe qui. Cette approche n'est pas tout à fait nouvelle (modèle ASP, IBM on demande). La réelle nouveauté réside dans son approche systématique. [1]

Le Cloud permet un accès facile et à la demande par le réseau à un ensemble partagé de ressources informatiques configurables (serveurs, stockage, applications et services) qui peuvent être rapidement provisionnées et libérées par un minimum d'efforts de gestion ou d'interaction avec le fournisseur du service. [2]

Le Cloud Computing couplé, aux technologies de virtualisation, permet la mise à disposition d'infrastructures et de plate-forme à la demande. Mais le Cloud Computing ne concerne pas seulement l'infrastructure (IaaS), il bouleverse la plate-forme d'exécution (PaaS) et les applications (SaaS) : Comme nous le verrons plus loin, le Cloud est à la fois transversal et vertical. [1]

Le Cloud a occupé le devant de la scène durant une grande partie de l'année 2010 et bon nombre d'analystes annoncent que 2011 sera l'année du Cloud. [3]

Basiquement, le Cloud propose trois couches :

- ✓ L'infrastructure (IaaS : Infrastructure as a Service)
- ✓ La plate-forme (PaaS : Platform as a Service)
- ✓ L'application (SaaS : Software as a Service)

En clair, le Cloud Computing c'est :

- ✓ L'informatique « comme un service », c'est-à-dire à la demande
- ✓ Souvent basé sur de la virtualisation (surtout pour l'IaaS et le PaaS)

Trois couches :

- ✓ Infrastructure.
- ✓ Plateforme.
- ✓ Applicative.

Du « self-service » avec un paiement à la consommation (je paye ce que je consomme).

Abstraction, mutualisation et allocation dynamique des ressources physiques.

2. Origine du Cloud Computing

Le premier nuage était construit autour du réseau (abstraction TCP/IP). Le deuxième nuage était celui des documents (abstraction du World Wide Web). Le nuage actuel, Cloud Computing, est une abstraction de l'infrastructure informatique qui masque la complexité des serveurs, des applications, des données et des plates-formes hétérogènes. La traduction en français du terme Cloud Computing n'est pas simple. Informatique en nuage ou infonuagique comme le tentent nos amis canadiens ne semblent pas promis à une grande carrière. Dans cet article, je conserverai le terme original "Cloud Computing". [2]

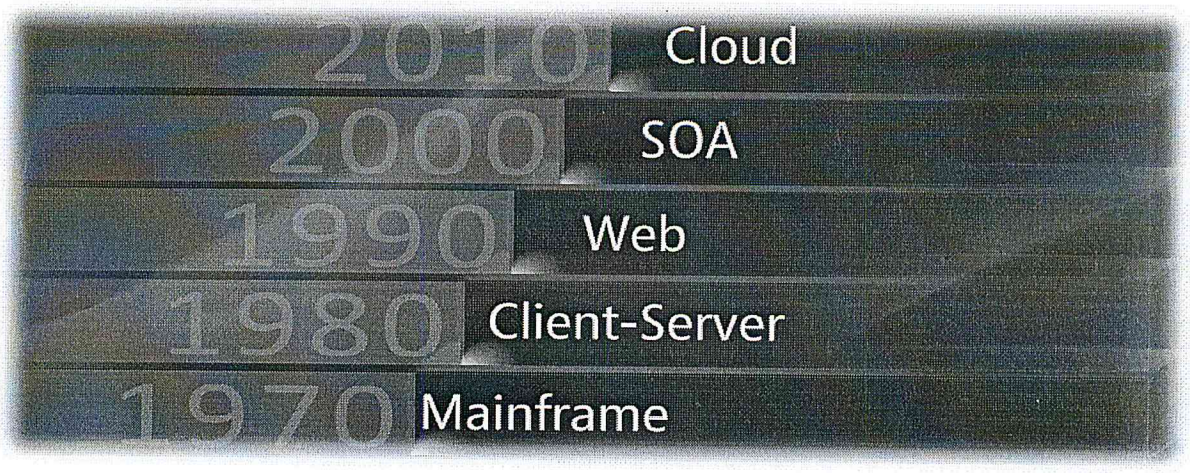


Figure 1 : 5eme génération d'architecture [4]

3. Caractéristiques et avantages du Cloud Computing :

Le Cloud Computing a pour but d'offrir des services qui vont au-delà de ces offres classiques et que nous pouvons tenter de définir avec les caractéristiques suivantes :

- Ils s'agit d'une informatique distribuée où les échanges sont gérés et centralisés par des serveurs distants, les applications étant stockées non plus sur le poste de travail, mais sur un "nuage" (Cloud) de serveurs, accédées par une connexion Internet et un navigateur web.
- Les applications, plateformes et infrastructures nécessaires sont louées en fonction de l'usage qui en est fait, que ce soit pendant le développement de ces applications ou pendant leurs utilisations en production.
- Les applications, plateformes et infrastructures sont facilement extensibles.
- Les ressources peuvent être allouées dynamiquement en fonction du besoin.
- Les applications, plateformes et infrastructures restent disponibles en cas de panne d'une ressource.

Cette configuration modifie radicalement la façon dont les informations et les ressources technologiques sont gérées et provisionnées dans l'entreprise:

- **Efficacité :** Les ressources d'un Cloud ne sont pas dépendantes d'un périphérique et ne sont pas rattachées à un emplacement. Un serveur dédié à chaque application n'est plus nécessaire : les ressources virtualisée peuvent résider n'importe où (et ni le programmeur ni

l'utilisateur n'a à se préoccuper de savoir où). Résultat : les économies d'échelle et les taux d'utilisation augmentent, avec un matériel moins important et consolidé.

• **Flexibilité :** Celle-ci est liée à deux avantages qu'offre le Cloud. Des ressources de tous types, logicielles ou matérielles, peuvent être assemblées pour créer de nouveaux systèmes d'informations, de nouvelles configurations et fonctions métiers, avec une rapidité sans précédent.

En outre, il est possible d'affecter des ressources technologiques supplémentaires lorsque nécessaire pour faire face aux pics d'activité, puis de les libérer une fois la charge ramenée à la normale. En d'autres termes, toutes les ressources voulues peuvent être très rapidement mobilisées « là où se déroule l'action », plus que jamais auparavant.

• **Accessibilité :** Un spectre beaucoup plus large d'informations, d'applications, de services technologiques et de services métiers est mis à la disposition de l'entreprise, de son personnel et de ses processus, en général via une interface de type navigateur standard.

• **Fiabilité :** Un Cloud peut présenter autant de redondance que le désire l'entreprise et peut mobiliser des ressources pour la sauvegarde et la restauration dès que nécessaire, sans nécessiter de configurations matérielles parallèles.

• **Sécurité :** Les ressources peuvent être protégées non pas uniquement par le pare-feu périphérique et le cryptage des informations, mais aussi localement, par l'intégration de règles métiers dans les conteneurs virtuels, en particulier pour les informations les plus sensibles.

• **Automatisation :** Le logiciel de gestion des ressources d'un Cloud agit comme un « agent de la circulation » automatique, déterminant de façon dynamique ce qui va où, et comment les ressources sont exploitées. La charge de travail journalière de l'équipe informatique est ainsi réduite, et les décisions quant à l'utilisation des ressources sont plus cohérentes.

• **Optimisation :** Étant donné qu'un Cloud est géré globalement, il est plus facile d'optimiser ses ressources collectivement, afin de parvenir à un équilibre idéal entre capacités, performances et coûts pour l'entreprise. [5]

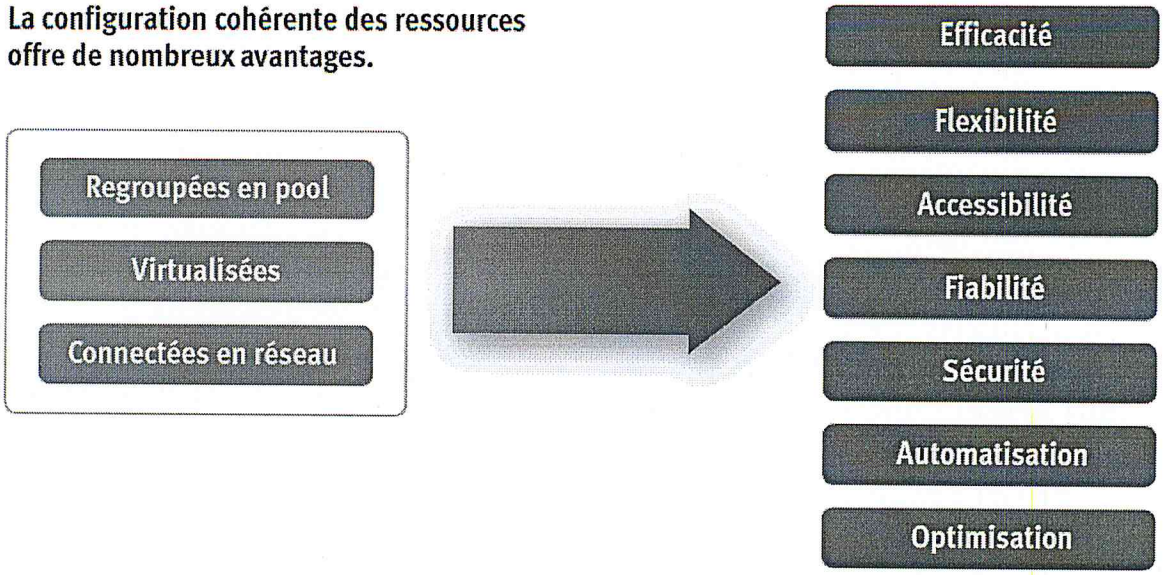


Figure 2 : la configuration cohérente des ressources offre de nombreux avantages. [5]

4. Inconvénients Cloud Computing :

• **sécurité** : la plateforme Cloud, si elle est externe (non installée sur le réseau interne ou avec une ouverture extérieure) doit être suffisamment sécurisée pour éviter le risque d'intrusion, de vol des données par piratage. L'autre risque est qu'un utilisateur oublie de se déconnecter sur un appareil accessible par des éléments externes à l'organisation. Il faut dans ce cas prévoir une déconnexion automatique en cas de non-activité du compte et bien segmenter les droits utilisateurs afin que ces derniers ne puissent accéder qu'aux données des projets dans lesquels ils sont impliqués. Plus généralement, une clause de confidentialité et la confiance dans son personnel sont primordiales pour que les données ne fuitent pas de manière volontaire.

• **connexion :** c'est l'autre goulot d'étranglement. Si l'utilisateur n'a pas de connexion internet, ou une connexion insuffisante, il ne pourra accéder à sa plateforme de travail. L'idée dans ce cas est de permettre le travail sur une application locale qui synchronise ensuite les données avec le serveur dès que l'utilisateur a à nouveau accès au réseau. Le problème de la sécurité des données en local se pose donc à nouveau.

La sauvegarde automatique des données et de niveaux de sécurité élevée n'étant pas garantis, il convient d'êtres très attentifs. [6]

5. Coûts et structure de coûts :

Outre une réduction des coûts directs, le Cloud permet de réaliser des économies et améliore la structure de coûts. La réduction des coûts à court terme provient en grande partie de la consolidation du matériel et de la virtualisation des ressources numériques. Les entreprises constatent une baisse globale de 40 % des coûts des Datacenter, notamment une baisse de 30 % des coûts de consommation électrique et de ventilation. Cette réduction de l'empreinte carbone jette les bases de l'informatique écologique. En règle générale, les Datacenter sont suréquipés pour pouvoir faire face aux pics de demande, alors que seulement 10 à 15 % des capacités sont régulièrement utilisés. La virtualisation permet un dimensionnement plus efficace du Datacenter, c'est-à-dire compte tenu de la capacité moyenne plutôt que du scénario le plus pessimiste. Et lorsque la charge augmente, les ressources sont automatiquement mises au service des activités métiers les plus importantes.

Dans la mesure où les grandes entreprises n'ont pas fini de consolider, de virtualiser et d'automatiser la gestion des ressources technologiques, elles ne sont pas encore en mesure d'apprécier la réduction de coûts généralisée offerte par le Cloud privé une fois celui-ci totalement déployé. L'efficacité opérationnelle obtenue, notamment au travers de processus de gestion des ressources à la fois flexibles, dynamiques et sans intervention manuelle, permet de faire baisser les coûts de 30 %.

Grâce au pooling et à la gestion centralisée des ressources, le Cloud privé procure des économies d'échelle, améliore l'utilisation des ressources, limite les dépenses d'investissement, accroît durablement l'efficacité opérationnelle et convertit des coûts fixes en coûts variables (vous ne payez que pour les services du Cloud public consommés). [5]

6. Les modèles de services :

6.1 Infrastructure as a Service (IaaS):

Les IaaS (Infrastructure as a Service) fournissent aux développeurs les briques fondamentales à la base des applications web: serveurs physiques, espace de stockage (disques durs), ressources réseaux (bande passante), mémoire (RAM) qui peuvent en disposer comme bon leur semble. Au lieu de devoir acheter ces ressources physiques pour

faire tourner leurs applications, les développeurs les louent et les configurent en temps réel suivant leurs besoins.

Il y a quelques années pour faire tourner leurs applications web les entreprises avaient deux solutions: soit acheter leurs propres serveurs soit loué des serveurs à des spécialistes qui s'occupaient alors du matériel (dans des Datacenter). Si ces deux solutions ont encore leurs avantages, force est de constater que la flexibilité n'est pas leur force première et qu'elles ne sont pas adaptées à toutes les entreprises:

- **hébergement propre**: nécessité de compétences internes pour gérer les serveurs, coûts fixes élevés. Davantage pertinent pour les grosses entreprises avec de gros trafics.
- **location de serveurs:** en général les hébergeurs offrent des solutions peu flexibles. Pour un abonnement fixe par mois vous disposez d'un espace de stockage et de ressources fixes (mémoire, serveurs, bande passante). Cette configuration ne s'adapte pas dynamiquement aux besoins de trafic du site (pics de trafic) et ces ressources sont sous utilisées la plupart du temps.

Les plateformes IaaS ont permis aux développeurs de prendre la main sur ces ressources et de les louer à la volée. Si vous avez besoin d'une certaine quantité de bande passante à midi mais que votre trafic est bien supérieur en début de soirée au lieu d'être contraint par des ressources fixes vous pouvez ajuster vos besoins suivant votre trafic. De plus vous ne payez que ce que vous consommez, là où l'hébergement était un coût fixe il devient un coût variable. Ce modèle est d'ailleurs de plus en plus adopté par les hébergeurs traditionnels qui proposent des offres de ce type.

Un des précurseurs des IaaS est Amazon qui est maintenant le leader des plateformes IaaS avec Amazon Web Service. Deux des services les plus connus étant EC2 et S3.

Amazon EC2 (Elastic Compute Cloud) est un service d'Amazon qui permet justement aux développeurs de disposer et de configurer ces ressources informatiques suivant leurs besoins. Le principe de base est relativement simple: le développeur peut créer des briques appelées des "instances EC2", une instance EC2 étant une configuration particulière de ressources : une certaine taille mémoire (RAM), une puissance de calcul, un choix d'OS (windows server, Linux, Oracle etc...), une taille d'espace de stockage.

Ainsi si votre application doit traiter énormément de données vous pouvez privilégier une grosse puissance de calcul, s'il y a beaucoup d'échanges de données vous privilégierez la mémoire etc... Chaque instance EC2 peut être configurée finement par le développeur qui peut aussi les multiplier en fonction de l'importance du trafic. Le développeur a la main sur ces ressources et peut les allouer et les libérer en temps réel.

Amazon S3 est le service de stockage d'Amazon. Au lieu d'acheter des disques durs, grâce à Amazon S3 l'utilisateur peut consommer exactement l'espace de stockage dont il a besoin. Si son besoin augmente il achète davantage d'espace et si au contraire il diminue il peut libérer de l'espace et payer moins. L'utilisateur n'a pas à se soucier de planifier ses besoins, l'espace est disponible à la demande et en temps réel.

6.2. Plateforme as a Service (PaaS):

Les PaaS (Platform as a Service) opèrent sur la couche supérieure des IaaS. Les IaaS permettent aux développeurs de configurer leur infrastructure (configuration du hardware) et d'en disposer de façon flexible mais la gestion virtuelle de ces ressources reste une tâche à part entière et beaucoup de développeurs ne peuvent/veulent pas s'y atteler. Leur objectif est de se concentrer sur leur application et non sur les infrastructures nécessaires (invisibles à l'utilisateur final).

Les PaaS sont des plateformes construites sur des IaaS et qui y ajoutent une couche de services qui facilite le déploiement et l'exécution des applications dans le Cloud. Pour déployer une application un développeur n'a pas uniquement besoin d'espace de stockage, de mémoire et de capacité serveur, il a besoin d'un environnement d'exécution qui fait tourner l'application suivant le langage de programmation (qui n'est pas le même s'il s'agit de Java, de php, de Python, de Ruby etc...), le choix du type de base de données (SQL, du noSQL...), de librairies de programmation, des outils de test, de monitoring etc.... C'est tout cet environnement (et sa configuration) que les PaaS offrent aux développeurs. De même grâce à ces plateformes le développeur n'a pas à s'occuper de "l'entretien" de son environnement d'exécution (patches de sécurité, mises à jour, nouvelles fonctionnalités...).

C'est pour ces raisons qu'il n'existe pas encore de PaaS universelle, chaque PaaS est plus ou moins tournée vers une communauté spécifique: Heroku (construite sur les services IaaS d'Amazon) était au départ dédiée à la communauté Ruby, Google App Engine propose

des environnements pour le Java et Python, Microsoft Azure pour du .NET etc... Mais de nouvelles PaaS arrivent sur le marché et se spécialisent sur des niches spécifiques comme force.com qui est une PaaS dédiée aux utilisateurs de SalesForce.

Les avantages procurés par les PaaS sont donc nombreux: gestion automatique de la partie infrastructure (comme avec une IaaS), de l'environnement d'exécution, facilitation du déploiement d'applications etc... Les développeurs peuvent se concentrer sur la création de leur application web et accélérer les cycles de développement, abaissant sérieusement les barrières d'entrées (autant financières, de compétences ou de temps).

Le désavantage principal est qu'une fois l'application déployée sur une PaaS le développeur devient prisonnier de la plateforme choisie et tributaire des choix du gestionnaire de celle-ci.

6.3. Software as a Service (SaaS):

Si vous avez suivi jusqu'ici l'article vous aurez sûrement compris que les IaaS et PaaS étaient dédiées aux développeurs et que les SaaS constituaient le dernier étage de la fusée, celle destinée aux utilisateurs finaux.

Les SaaS (Software as a Service) sont les applications construites sur les infrastructures Cloud (IaaS et PaaS) et accessibles via internet aux utilisateurs finaux. Il existe de nombreux types de SaaS qui vont de webmails (gmail, hotmail) aux solutions de CRM en ligne (Zoho, Salesforce) en passant par des outils de productivité (la série des Basecamp, HighRise etc.).

Les SaaS sont des logiciels dans le Cloud et les différences que cette approche implique sont multiples.

Tout d'abord sur le modèle de consommation des logiciels. Dans le modèle traditionnel du logiciel le client achetait un logiciel et en devenait le propriétaire, son utilisation était illimitée, en revanche il devait payer pour les mises à jour ou les nouvelles versions qui sortaient. Le modèle est tout autre pour le SaaS. Ici l'application (le logiciel) est accédé comme s'il s'agissait d'un service, le client paye un abonnement mensuel/annuel (par utilisateur ou global) et les mises à jour sont gratuites et déployées de façon invisible pour l'utilisateur (pas de mise à jour à effectuer lui-même).

Second point différenciant l'accès aux applications et aux données. Les logiciels traditionnels ne sont en général accessibles que sur les postes sur lesquels ils ont été

installés. Pas possible d'accéder à Outlook express sur son téléphone portable par exemple. Grâce au SaaS cet accès est facilité puisqu'il s'effectue directement depuis le navigateur internet ou un client léger à télécharger (une application mobile par exemple).

Les avantages du modèle SaaS par rapport au modèle logiciel traditionnel.

Pour l'utilisateur final:

- accès à l'application et aux données n' importe où (PC, smartphone, tablette) et n'importe quand
- pas de gestion de la mise à jour du logiciel (directement effectuée par le développeur du SaaS)
- pas de gestion de la sécurité du côté logiciel de la part de l'utilisateur final (les patches de sécurité et de mise à jour sont déployés par le développeur du SaaS)
- plus de flexibilité dans les coûts (possibilité d'ajouter ou de supprimer des utilisateurs d'un mois à l'aute)

Pour le développeur:

- cycles de développement plus courts (nouvelles fonctionnalités plus rapidement mises en place)
- possibilité de mettre en place des indicateurs qui mesurent l'utilisation réelle de leur solution pour mieux répondre aux besoins de l'utilisateur final. [7]

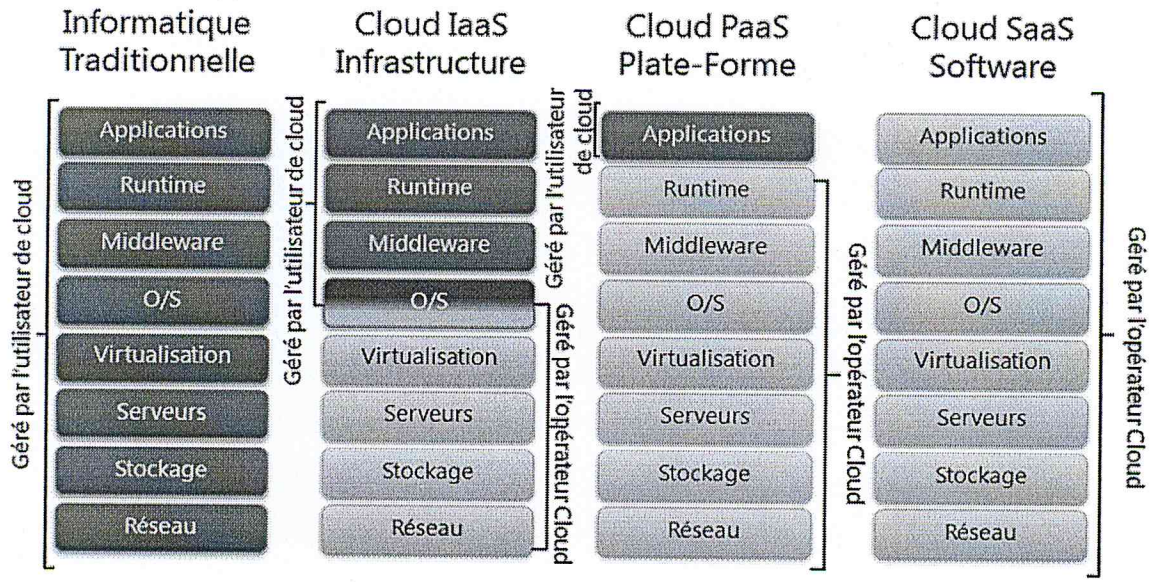


Figure 3 : Les différents modèles de services de Cloud Computing. [12]

7. Les modèles de déploiement :

Certains distinguent quatre modèles de déploiement. Nous les citons ci-après bien que ces modèles n'aient que peu d'influence sur les caractéristiques techniques des systèmes déployées.

7.1 Cloud public:

L'infrastructure Cloud est ouverte au public ou à de grands groupes industriels. Cette infrastructure est possédée par une organisation qui vend des services Cloud. C'est le cas le plus courant. C'est celui de la plate-forme Amazon Web Services déjà citée. [9]

7.2. Cloud privé:

L'infrastructure Cloud est utilisée par une seule organisation. Elle peut être gérée par l'organisation ou par une tierce partie. L'infrastructure peut être placée dans les locaux de l'organisation ou à l'extérieur. [9]

La différence entre un Cloud privé (Privat Cloud) et public (public Cloud)?

La différence entre un Cloud privé et un Cloud public est simple. Dans le cas d'un Cloud public l'infrastructure Cloud est utilisée par de différentes entreprises ; dans le cas d'un Cloud privé l'infrastructure Cloud est utilisée par une seule entreprise.

Dans le cas de Cloud public vous payez seulement pour les ressources et services que vous utilisez réellement. Des utilisateurs peuvent facilement adapter des serveurs ou installer de nouveaux serveurs. Ils ne doivent pas non plus investir en matériel. Le fournisseur du Cloud public prend soin à ce qu'il y ait suffisamment de capacité à l'intérieur du Cloud.

Dans le cas d'un Cloud privé, le Cloud n'est pas partagé hors de l'entreprise. Le groupe de matériel installé peut seulement être utilisé par cette entreprise. Lorsque vous avez besoin de capacité supplémentaire, un matériel supplémentaire (un nœud) sera ajouté au groupe.

Un Cloud privé est utile à des entreprises plus grandes ou à des entreprises avec beaucoup de serveurs ou lorsqu'il y a des règles de sécurité spécifiques que des Cloud publics ne peuvent pas offrir.

Les avantages Cloud privé :

- Nous avvons le contrôle complet sans restrictions.
- C'est plus sûr puisque nous sommes le seul à utiliser ce Cloud et nous pouvons donc déterminer nous-même tous les paramètres de sécurité.
- C'est plus flexible, vous installez des serveurs virtuels lorsque nous en avons besoin.
- C'est plus performant: les ressources matérielles sont garanties. [11]

7.3. Cloud hybride :

L'informatique hybride résulte d'une combinaison entre le Cloud privé (interne) et le Cloud public (externe). Cette nouvelle solution offre aux dirigeants d'entreprises l'avantage de mettre en place des Cloud internes pour aboutir au niveau de sécurité requis par l'intégration d'un certain nombre de processus managériaux. Et ce, tout en assurant la disponibilité nécessaire pour l'hébergement d'applications critiques, et de recourir en même temps au Cloud Computing, pour l'hébergement des applications, services et données qu'ils estiment non critiques. En effet, l'informatique hybride permet aux entreprises de fournir à leur clientèle la possibilité de s'approvisionner d'un Cloud public et garantir, par la même occasion, un niveau de sécurité optimal par l'adoption d'un Cloud privé. Il s'agit d'une solution plus souple, pratique et économique, en termes de gestion.

L'informatique hybride constitue une solution très avantageuse pour les dirigeants d'entreprises

Le Cloud hybride est une solution plus appropriée car, étant le fruit d'une combinaison entre le Cloud public et le Cloud privé, il permet de compenser le réseau ou nuage interne par le réseau, ou nuage externe et inversement.

Cette solution correspond parfaitement aux attentes et besoins actuels de la plupart des dirigeants d'entreprises, dans la mesure où elle répond aux soucis de sécurisation des données gérées, échangées ou conservées, ainsi qu'au respect du principe de la

confidentialité (Cloud privé), tout en offrant l'opportunité de bénéficier d'un Cloud Computing au sens propre du terme (Cloud public). [12]

7.4. Cloud communautaire :

L'infrastructure Cloud est partagée par plusieurs organisations pour les besoins d'une communauté qui souhaite mettre en commun des moyens (sécurité, conformité, etc..).

Elle peut être gérée par les organisations ou par une tierce partie et peut être placée dans les locaux ou à l'extérieur. [9]

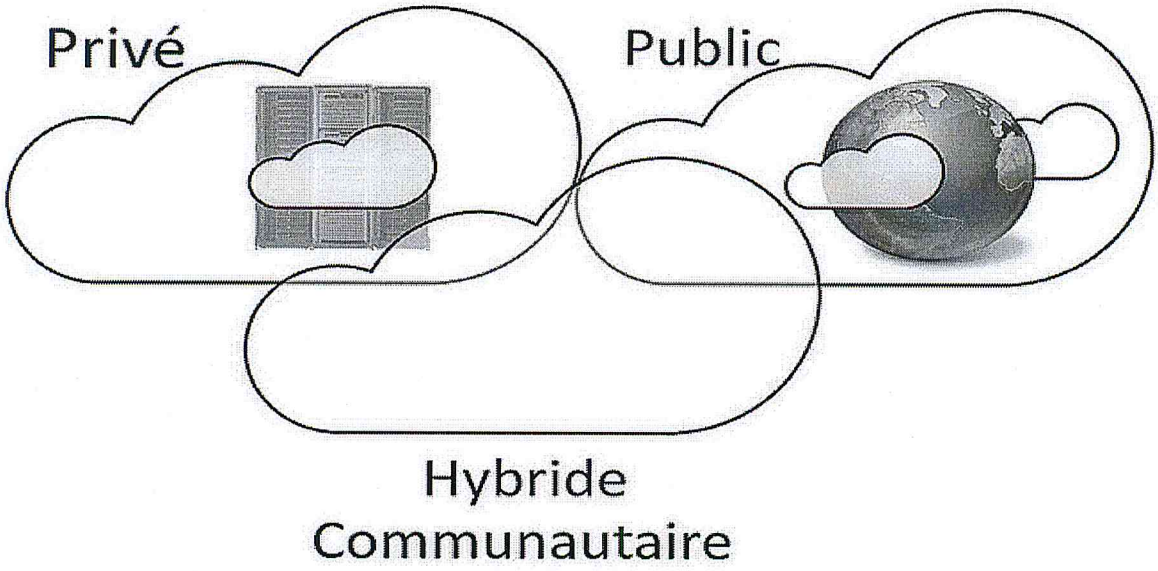


Figure 4 : Modèle de déploiement de Cloud Computing [10]

8. Conclusion :

Le Cloud Computing est donc un moyen de délivrer un service informatique ciblé et quantifié à une clientèle précise sans que cette dernière n'ait à investir dans un système d'information dédié à ce service. Selon cette définition, nous avons vu des modèles de déploiement tels que le privé, public, hybride, communautaire ; et des modèles de service tels que le PaaS, SaaS, IaaS.

Ces modèles reposent sur des technologies de virtualisation qui permettent d'atteindre la flexibilité requise à la réalisation de ces modèles. La virtualisation est une technologie clé du Cloud Computing. Nous allons détailler cette technologie dans le chapitre suivant.

Introduction :

Les technologies dites de « virtualisation » ont connu un essor important ces dernières années, lié notamment au développement de nouveaux usages comme l'informatique en nuage (Cloud Computing). Virtualiser un ensemble de serveurs est devenu aujourd'hui relativement aisé, et de nombreuses entreprises ont choisi de « virtualiser » leurs serveurs pour faire des économies de place, d'énergie et de budget.

La virtualisation apparaît comme étant une solution clé pour révolutionner l'architecture ossifiée des réseaux comme Internet. En ajoutant une couche d'abstraction au-dessus du matériel, la virtualisation permet de gérer et de configurer des réseaux virtuels indépendamment les uns des autres. La flexibilité qui en résulte donne à l'opérateur d'un réseau virtuel la possibilité de configurer la topologie, et de modifier les piles protocolaires. Jusqu'à présent, la virtualisation du réseau a été implémentée dans des plateformes de test ou de recherche, pour permettre l'expérimentation avec les protocoles de routage. Dans le but d'introduire la virtualisation dans les réseaux de production comme ceux de l'Internet, plusieurs nouveaux défis apparaissent, dont en particulier la performance et le partage des ressources de commutation et de routage.

1. Définition :

La virtualisation est comme l'ensemble des techniques matérielles et/ou logiciels qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation et/ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes. Il s'agit donc d'utiliser une seule machine physique en remplacement de plusieurs et d'utiliser les possibilités offertes par la virtualisation pour démultiplier le nombre de machines virtuelles. [14]

Ainsi, la virtualisation aide les départements informatiques à réduire les coûts et à renforcer la continuité métier. Les solutions Microsoft couvrent à la fois les infrastructures physique et virtuelle, et se gèrent très facilement à partir d'une console unique. [15]

À l'origine, le matériel informatique dont nous disposons actuellement a été conçu pour n'exécuter qu'un seul système d'exploitation et qu'une seule application. La virtualisation

dépasse ces limites en permettant d'exécuter simultanément plusieurs systèmes d'exploitation et plusieurs applications sur le même ordinateur, ce qui accroît l'utilisation et la flexibilité du matériel. La virtualisation est une technologie dont peut bénéficier toute personne qui utilise un ordinateur, qu'il s'agisse des professionnels de l'informatique, des entreprises, des organismes publics et même des particuliers. Plusieurs machines virtuelles partagent des ressources matérielles sans interférer entre elles, ce qui vous permet d'exécuter en toute sécurité plusieurs systèmes d'exploitation et applications en simultané sur un seul et même ordinateur. [16]

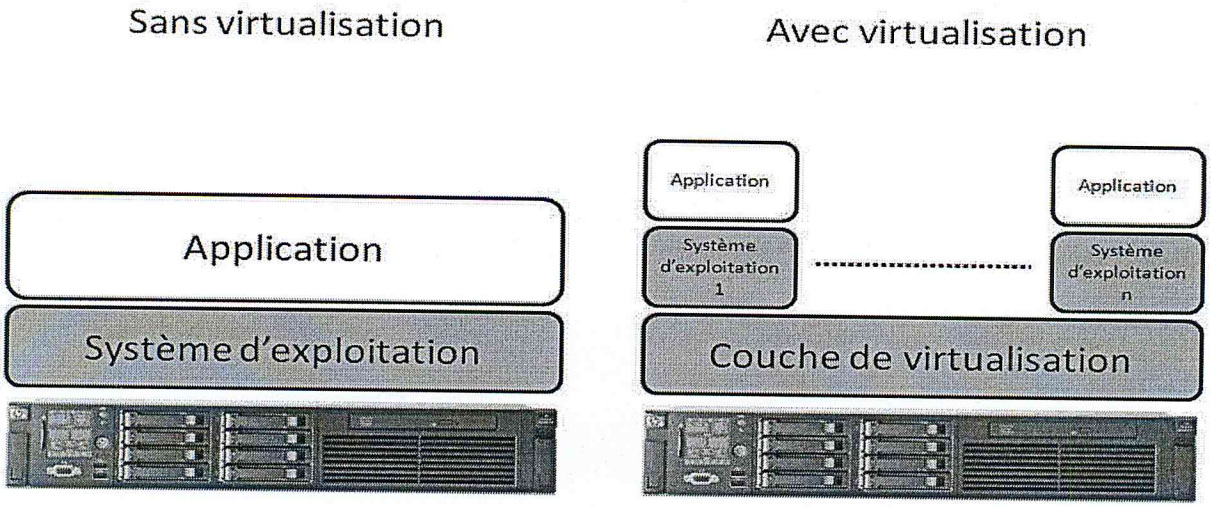


Figure 5 : Différence entre architecture standard et virtualisée [17]

Sans virtualisation, un seul système peut être opérationnel sur une machine physique alors qu'avec la virtualisation, il est possible d'en faire fonctionner plusieurs.
La couche de virtualisation appelée hyperviseur masque les ressources physiques d'un équipement matériel pour proposer à un système d'exploitation des ressources différentes de ce qu'elles sont en réalité. Elle permet en outre de rendre totalement indépendant un système d'exploitation du matériel sur lequel il est installé, ce qui ouvre de grandes possibilités.

Le concept de virtualisation n'est pas nouveau puisqu'il a été inventé par IBM avec les grands systèmes *Mainframe* à la fin des années 1970. VMware a su adapter cette technologie aux environnements x861 en 1998. Il existe plusieurs formes de virtualisation : serveurs, applications, poste de travail... [17]

2. Historique :

C'est en France, dans les laboratoires d'IBM, à Grenoble, que les premiers travaux sur les machines virtuelles font leur apparition. Nous sommes alors en 1960 et Big Blue vient de créer son premier ordinateur avec une base logicielle commune, le System/360, qui pour la première fois n'obligera pas à changer tout le matériel (imprimante, carte. . .) lors de la prochaine évolution du processeur. Cela permettra également de conserver les programmes, sans avoir à en réécrire spécifiquement des parties. Cette première évolution sera continuée par la naissance du CP-40, considérée comme la première machine virtuelle. Le produit se transforma en VM/CMS. La suite logique donnée par IBM les conduira vers les mainframes qui virtualisent leur système d'exploitation. IBM étant à l'époque un vendeur de matériel, il ne pouvait alors pas faire davantage la promotion d'une technologie qui aurait permis au client d'économiser sur ses ventes. Par la suite, d'autres sociétés comme HP, avec ses PA-RISC ou IA64, ou encore Sun avec la série des E10K/E15K/E20K/E25K utiliseront la technologie de virtualisation.

Le système commercial le plus connu actuellement se nomme VMware, du même nom que la société qui le commercialise. C'est cette société qui popularisera auprès du grand public l'intérêt des machines virtuelles, que ce soit pour des tests ou de la production.

De nombreux outils libres et propriétaires existent aujourd'hui, nous en citeront quelques-uns pour nous attarder plus particulièrement sur VMware Infrastructure 3, l'outil de virtualisation orienté production, commercialisé par la société VMware. [18]

3. Intérêt de la virtualisation :

Les outils de virtualisation permettent de faire fonctionner ce que l'on appelle des environnements virtuels. Les entreprises y ont de plus en plus recours à car elle leur permet de gagner de la place dans les salles serveurs, de faciliter les installations et les redémarrages après incidents, et de sécuriser les systèmes.

La virtualisation présente un grand nombre d'intérêts pour les entreprises :

- **utilisation optimale des ressources** d'un parc de machines (répartition des machines virtuelles sur des machines physique en fonction des charges respectives) ;

- **installation, déploiement et migration facile** des machines virtuelles d'une machine physique à une autre ;
- **économie sur le matériel** par mutualisation (consommation électrique, entretient physique, monitoring, support...) ;
- **sécurisation** et/ou **isolation** d'un réseau (cassage des systèmes d'exploitation virtuels, mais pas des systèmes d'exploitation hôtes qui sont invisibles pour l'attaquant) ;
- **diminution des risques** liés au dimensionnement des serveurs lors de la définition de l'architecture d'une application, l'ajout de puissance (nouveau serveur par exemple) étant alors transparente.

La virtualisation possède également des intérêts pédagogiques :

- **simplicité** : pouvoir simuler un réseau sur une machine sans avoir besoin d'autant de machines qu'il y a d'hôtes sur le réseau simulé ;
- **possibilité de simuler le fonctionnement de réseaux complexes** (sous réserve de ressources matérielles suffisantes).

Chaque outil de virtualisation implémente une ou plusieurs de ces notions :

- **couche d'abstraction** matérielle et/ou logicielle ;
- **systèmes d'exploitations** (ou applications) « virtualisée(s) » ou « invité(s) » ;
- **partitionnement, isolation** et/ou **partage** des ressources physiques et/ou logicielles ;
- **images manipulables** : démarrage, arrêt, clonage, sauvegarde et restauration, migration d'une machine physique à une autre ;
- **réseau virtuel** : réseau purement logiciel, interne, à la machine hôte, entre hôte et/ou invité. [19]

4. Avantage de la virtualisation :

- **Consolidation des serveurs et optimisation de l'infrastructure.**

La virtualisation permet d'accroître considérablement le taux d'utilisation des ressources grâce à l'allocation dynamique de la puissance de calcul en fonction des besoins de chaque application à un instant donné (en regroupant des ressources communes on sort du schéma « une application = un serveur »)

- **Réduction des coûts de l'infrastructure physique.**

Avec la virtualisation, nous pouvons réduire le nombre de serveurs et la quantité de matériel informatique nécessaires dans le centre de données. Cela se traduit par une

diminution des frais immobiliers et des besoins en alimentation et en ventilation, entraînant une nette réduction des coûts informatiques.

- **Augmentation de la flexibilité et de l'efficacité opérationnelle.**

La virtualisation offre une nouvelle manière de gérer l'infrastructure informatique et peut aider les administrateurs informatiques à consacrer moins de temps aux tâches répétitives.

- **Installation, déploiement et migration facile des machines virtuelles d'une machine physique à une autre.**

Notamment dans le contexte d'une mise en production à partir d'un environnement de qualification ou de pré-production, livraison facilitée.

- **Disponibilité accrue des applications et amélioration de la continuité d'activité.**

Élimine les interruptions de service programmées et rétablissez rapidement le service en cas d'interruptions non programmées. Sauvegardez et déplacez en toute sécurité des environnements virtuels entiers sans interrompre le service.

- **Sécurisation et/ou isolation d'un réseau.** [20]

5. Inconvénients de la virtualisation :

- **Certains programmes n'acceptent pas la virtualisation.**

Tous les programmes ne sont pas conçus pour être virtualisée. Les programmes graphiques ou très gourmands en mémoire, ceux destinés aux multimédias ou aux calculs très complexes, demandent tous beaucoup de puissance. Il arrive que les MV n'en aient pas assez pour prendre en charge de telles tâches. Alors qu'une majorité de programmes peuvent tourner au sein d'une MV, certains ne peuvent simplement pas être exécutés « en streaming » depuis un serveur.

- **Des prises en charge de licence cauchemardesques.**

Certains vendeurs distribuent leurs licences aux utilisateurs, d'autres suivent les adresses MAC, d'autres encore le font en fonction du SE.

- **L'informatique est virtuelle mais les périphériques sont concrets.**
- **...**

Contrairement à la virtualisation de serveur (consistant à faire tourner plusieurs serveurs virtuels sur quelques serveurs réels seulement), cette astuce ne fonctionne pas avec les ordinateurs de bureau. Alors que vous pouvez faire tourner de nombreuses MV sur un même ordinateur de bureau, vous aurez encore besoin d'un ordinateur de bureau devant vous. Ce PC unique en indique maintenant une douzaine sur votre réseau. Donc, si vous pensez réduire drastiquement le nombre de vos machines, pensez-y à deux fois.

6. Les types de la virtualisation :

6.1. L'émulation :

Le logiciel de virtualisation crée un ordinateur virtuel simulé complet (Bios, processeur, mémoire, disque dur, cartes réseau, vidéo, ...), intercepte une grande majorité des instructions du système invité pour les remplacer par leur équivalent sur le système hôte. Cela permet d'exécuter des applications prévues pour d'autres architectures (ordinateurs, consoles, bornes d'arcade ...), mais le principale inconvénient sont les médiocres performances. [16]

6.2. La virtualisation complète ou « full virtualization » :

Ici le logiciel de virtualisation crée un ordinateur virtuel simulé complet (Bios, processeur, mémoire, disque dur, cartes réseau, vidéo, ...), intercepte et traduit uniquement certaines instructions particulières du système invité : celles qui auraient un impact en dehors de la machine virtuelle, ou ne peuvent être exécutées directement par l'hôte. Cela permet d'exécuter des applications prévues pour la même architecture (on ne peut pas avoir une VM pour architecture Intel X86 sur un PowerPC par exemple). Les performances s'améliorent considérablement avec le support de la virtualisation matérielle (Intel VT, AMD-V) de plus en plus souvent disponible. **[16]**

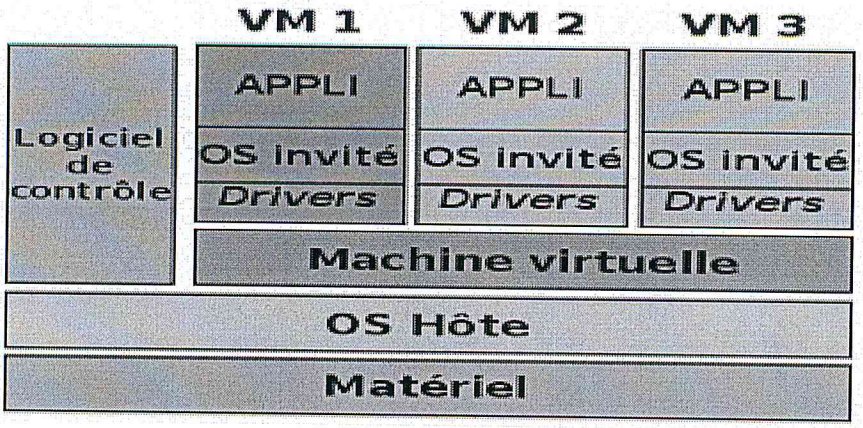


Figure 6 : La virtualisation complet [16]

6.3. La paravirtualisation :

La paravirtualisation fait intervenir un hyperviseur. Il s'agit d'un noyau allégé au-dessus duquel viendront se greffer les systèmes invités. Contrairement à un système traditionnel de machines virtuelles où la virtualisation est transparente, avec la paravirtualisation, le système invité doit avoir conscience qu'il tourne dans un environnement virtuel ce qui implique d'employer un noyau modifié. En termes de performances, la paravirtualisation offre des performances meilleures que les machines virtuelles. **[16]**

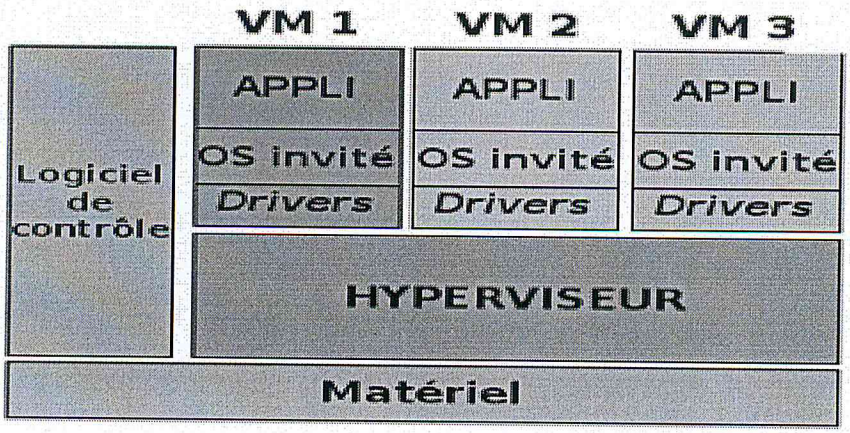


Figure 7 : La paravirtualisation [16]

7. Les domaines de la virtualisation :

7.1. La virtualisation d'applications :

La virtualisation d'application est une technologie logicielle qui va permettre d'améliorer la portabilité et la compatibilité des applications en les isolants du système d'exploitation sur lequel elles sont exécutées. Elle consiste à encapsuler l'application et son contexte d'exécution système dans un environnement cloisonné. La virtualisation d'application va nécessiter l'ajout d'une couche logicielle supplémentaire entre un programme donné et le système d'exploitation; son but est d'intercepter toutes les opérations d'accès ou de modification de fichiers ou de la base de registre1 afin de les rediriger de manière totalement transparente vers une localisation virtuelle (généralement un fichier). Puisque cette opération est transparente, l'application n'a pas notion de son état virtuel. Le terme virtualisation d'application est trompeur puisqu'il ne s'agit pas de virtualisée l'application mais plutôt le contexte au sein duquel elle s'exécute (registres du processeur, système de fichiers,...).

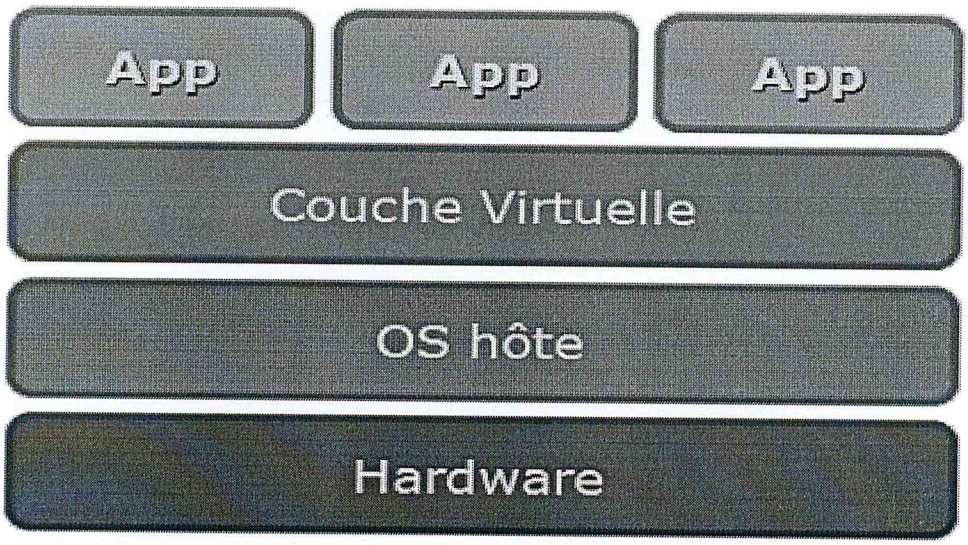


Figure 8 : Virtualisation d'applications [23]

Avantages Virtualisation d'applications :

Elle permet d'exécuter des applications qui ont été développées pour d'autres environnements d'exécution (p. ex.Wine permet d'exécuter des applications Windows sur une plateforme Linux) ; elle protège le système d'exploitation hôte en s'assurant que l'application virtualisée ne viendra pas interagir avec les fichiers de configuration du système; elle évite de faire appel à une machine virtuelle qui consomme plus de ressources ;

elle autorise l'exécution de code incorrect (p. ex. une application pourrait vouloir écrire un fichier dans un répertoire système dont elle ne possède que les droits en lecture). [23]

7.2. La virtualisation de réseau :

De manière générale, la virtualisation des réseaux consiste à partager une même infrastructure physique (débit des liens, ressources CPU des routeurs,...) au profit de plusieurs réseaux virtuels isolés. Un VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique. Puisqu'un VLAN est une entité logique, sa création et sa configuration sont réalisées de manière logicielle et non matérielle.

7.2.1. Les types de réseaux virtuels :

a- Les réseaux virtuels de niveau 1 :

Appelés réseaux virtuels par port (port-based VLAN) : ils définissent un réseau virtuel en fonction des ports de raccordement sur le commutateur (switch). Ainsi, chaque port du commutateur est associé à un réseau virtuel, indépendamment de la machine qui y est physiquement raccordée. Le principal inconvénient d'un VLAN de niveau 1 est sa rigidité : si une station se raccorde physiquement au réseau par l'intermédiaire d'un autre port du commutateur, alors il est nécessaire de reconfigurer ce commutateur afin de réintégrer la station dans le bon réseau virtuel.

b- Les réseaux virtuels de niveau 2 :

Appelés réseaux virtuels par adresse MAC (MAC address-based VLAN) : ils consistent à définir un réseau virtuel sur base des adresses MACdes stations. Une adresse MACest un identifiant unique implémenté dans chaque adaptateur réseau. Ce type de VLAN est beaucoup plus souple que le précédent car il est indépendant de la localisation de la machine.

c- Les réseaux virtuels de niveau 3 :

On distingue principalement deux types de VLAN de niveau 3 :

- **Les réseaux virtuels par adresse de sous-réseau (Network address-based VLAN) :** ils déterminent les réseaux virtuels sur base de l'adresse IP source des segments. Ce type de réseau virtuel est t'es flexible puisque les commutateurs adaptent automatiquement leur configuration lorsqu'une station est déplacée. En revanche, une légère dégradation des

performances peut se faire ressentir puisque les segments doivent être analysés plus minutieusement.

- **Les réseaux virtuels par protocole (Protocol-based VLAN) :** Dans ce cas, les réseaux virtuels sont créés sur base des protocoles utilisés (TCP/IP, IPX,...) et les stations sont regroupées en réseaux virtuels suivant le protocole qu'elles utilisent.

8.2.2 Les avantages les réseaux virtuels :

Une réduction du trac de diffusion (broadcast) puisque celui-ci est à présent contenu au sein de chaque réseau virtuel ; une sécurité accrue puisque l'information est encapsulée dans une couche supplémentaire ; une meilleure flexibilité puisqu'une modification de la structure des réseaux peut être réalisée en modifiant la configuration du commutateur. [23]

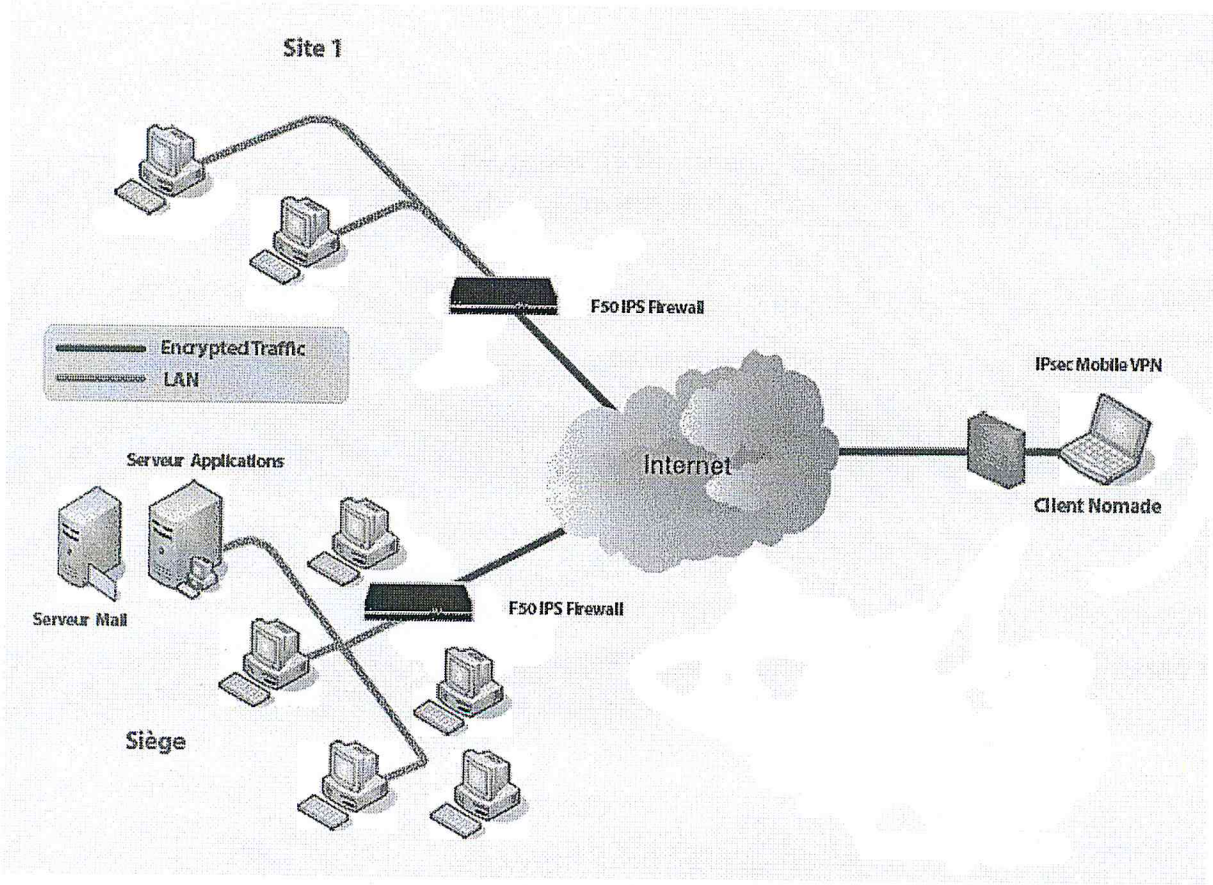


Figure 9 : Réseaux virtuels [22]

7.3. La virtualisation de stockage :

La virtualisation de stockage est un procédé qui va séparer la représentation logique et la réalité physique de l'espace de stockage. Son but est de faire abstraction des périphériques de stockage utilisés et des interfaces qui leur sont associés (SATA, SCSI,...) afin de limiter l'impact des modifications structurelles de l'architecture de stockage.

Ce type de virtualisation fait appel à une application d'administration de volumes logiques (Logical Volume Manager, LVM). Il s'agit d'une couche logicielle qui va permettre de regrouper plusieurs espaces de stockage, appelés volumes physiques, pour ensuite découper cet espace global suivant la demande en partitions virtuelles appelées volumes logiques. Ce processus de virtualisation peut être vu comme une extension du modèle de partitionnement classique des disques dur.

La virtualisation de stockage permet :

- d'adjoindre un périphérique de stockage supplémentaire sans interruption des services;
- de regrouper des unités de disques durs de différentes vitesses, de différentes tailles et de différents constructeurs ;
- de réallouer dynamiquement de l'espace de stockage. Ainsi, un serveur nécessitant un espace de stockage supplémentaire pourra rechercher des ressources non allouées sur le disque logique. Inversement, un serveur nécessitant moins d'espace de stockage pourra libérer cet espace et le rendre disponible pour d'autres serveurs. [23]

7.4. La virtualisation de serveurs :

La virtualisation des serveurs consiste à masquer les ressources du serveur, c.-à-d. le nombre et les caractéristiques de chaque machine physique, de chaque processeur et de chaque système d'exploitation pour les utilisateurs de ce serveur. L'administrateur du serveur va utiliser un logiciel grâce auquel il va diviser un serveur physique (constitué ou non de plusieurs machines distinctes) en plusieurs environnements virtuels isolés les uns des autres.

Ces environnements isolés sont parfois appelés serveurs privés virtuels, hôtes, instances, containeurs ou émulations. La virtualisation de serveurs s'inscrit dans une tendance globale qui tend à promouvoir la virtualisation au sein des entreprises en faisant notamment appel à la virtualisation de stockage et à la virtualisation de réseaux. Cette tendance est une composante dans le développement de systèmes autonomes. Un système

est dit autonome si il est capable de s'autogérer sur base de l'activité qu'il perçoit, sans aucune intervention externe, et en conservant les détails de son implémentation invisibles pour l'utilisateur. [23]

8. Différentes techniques de virtualisation :

Quatre techniques de virtualisation existent, les unes plus connues que les autres :

- Isolateur
- Noyau en espace utilisateur
- Machine virtuelle
- Hyperviseur
- Matériel

8.1. Isolateur :

Un isolateur c'est un logiciel qui confine les autres applications qu'on veut virtualiser dans des contextes propres à elles. On appelle aussi « zones d'exécution » cet espace mémoire spécifique à l'application virtualisée. Cette isolation permet d'avoir plusieurs instances d'une application initialement conçue pour n'exister qu'en mode instance unique.

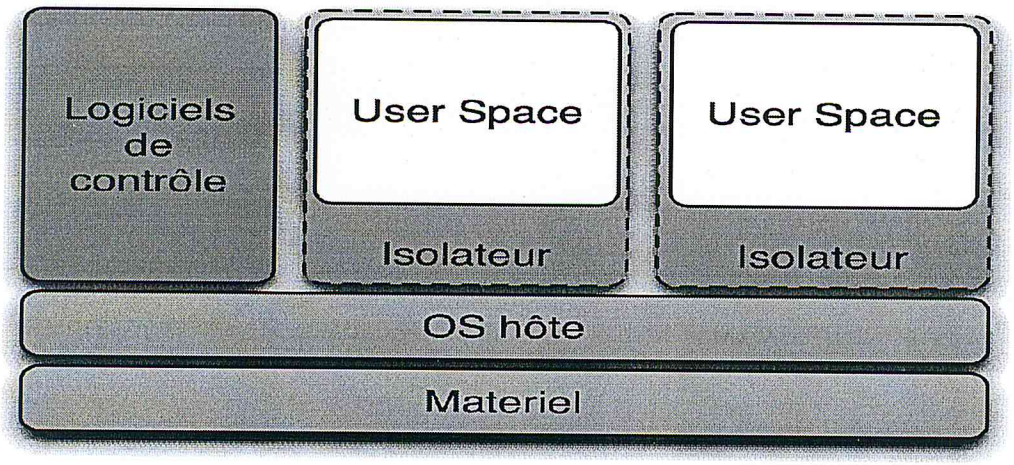


Figure 10 : Diagramme de l'architecture d'un isolateur [24]

On voit bien que l'isolation ne peut être utilisée pour virtualiser tout un système d'exploitation, mais en contrepartie il offre des performances supérieures. Autre limitation : les isolateurs sont surtout disponibles pour les systèmes linux. En voici quelques exemples :

- Linux-VServer : isolation des processus en user-space
- chroot : isolation changement de racine
- BSD Jail : isolation en user-space
- OpenVZ : libre, partionnement au niveau noyau sous Linux et Windows 2003

8.2. Noyau en espace utilisateur :

Dans cette situation, un noyau tourne comme une application dans l'espace utilisateur, ce qui lui donne son propre espace mémoire à gérer et lui permet le contrôle des applications. Cette méthode de virtualisation n'est pas très performante du fait que le système invité n'est pas tout à fait indépendant du système hôte. D'autre part, les deux noyaux empilés dans un même système physique ce qui rend les deux systèmes fortement dépendants.

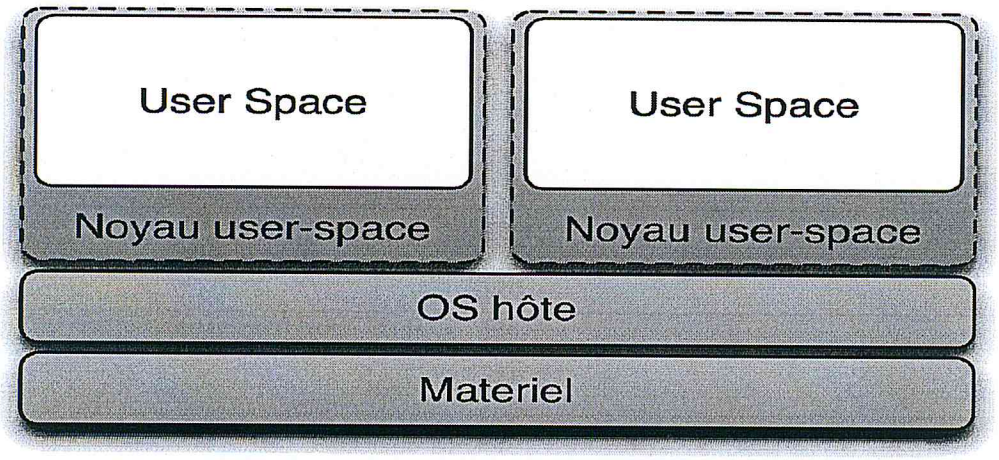


Figure 11 : Diagramme d'architecture du Noyau en espace utilisateur [24]

8.3. Machine virtuelle :

Un logiciel permet dans ce cas de lancer plusieurs OS invités sur la machine hôte. Ce logiciel émule un hardware que les machines invitées croient être celui de la machine hôte et donc directement communiquer avec ledit matériel. Par contre, la CPU (ou les CPUs) ainsi que la mémoire sont directement accessibles par les machines virtuelles, ce qui implique des performances plus intéressantes que dans le cas où une totale émulation aurait été faite.

Cette solution permet de faire cohabiter plusieurs systèmes d'exploitation complètement isolés. Ces derniers communiquent entre eux via les canaux systèmes

standards, et par réseau. En effet, toutes les machines virtuelles sont ou peuvent être dotées de cartes réseaux virtuelles qui sont en fait des buffers offrant la possibilité d'échanger des données avec l'extérieur.

Quelques exemples :

- QEMU : émulateur de plateformes x86, PPC, Sparc
- kvm : version modifiée de QEMU tirant parti des instructions de virtualisation des processeurs Intel et AMD (Intel VT ou AMD-V)
- Plex86 : émulateur de plateforme x86
- bochs : émulateur de plateforme x86
- PearPC: émulateur de plateforme PPC sur matériel x86
- VMware: propriétaire, émulateur de plateforme x86 (produits VMware Server, VMware Player et VMware Workstation). [24]

8.4. Hyperviseur :

Les hyperviseurs sont de plus en plus présents dans les architectures des entreprises étant donné que la virtualisation se développe et se répand rapidement. Les solutions sont multiples et plus ou moins coûteuses, mais, en ce qui concerne les hyperviseurs, il y en a deux types. Quoi qu'il en soit, votre serveur doit disposer d'une configuration matérielle supportant la technologie Intel-VT ou AMD-V pour pouvoir virtualiser.

Les types d'hyperviseur :

a. Hyperviseur de type 1 :

Un hyperviseur de type 1 est un système qui s'installe directement sur la couche matérielle du serveur. Ces systèmes sont allégés de manière à se « concentrer » sur la gestion des systèmes d'exploitation invités c'est-à-dire ceux utilisés par les machines virtuelles qu'ils contiennent. Ceci permet de libérer le plus de ressources possible pour les machines virtuelles. Toutefois, il est possible d'exécuter uniquement un hyperviseur à la fois sur un serveur. Parmi les hyperviseurs de type 1 on trouve des systèmes comme Xen, VMware ESX et Proxmox. [23]

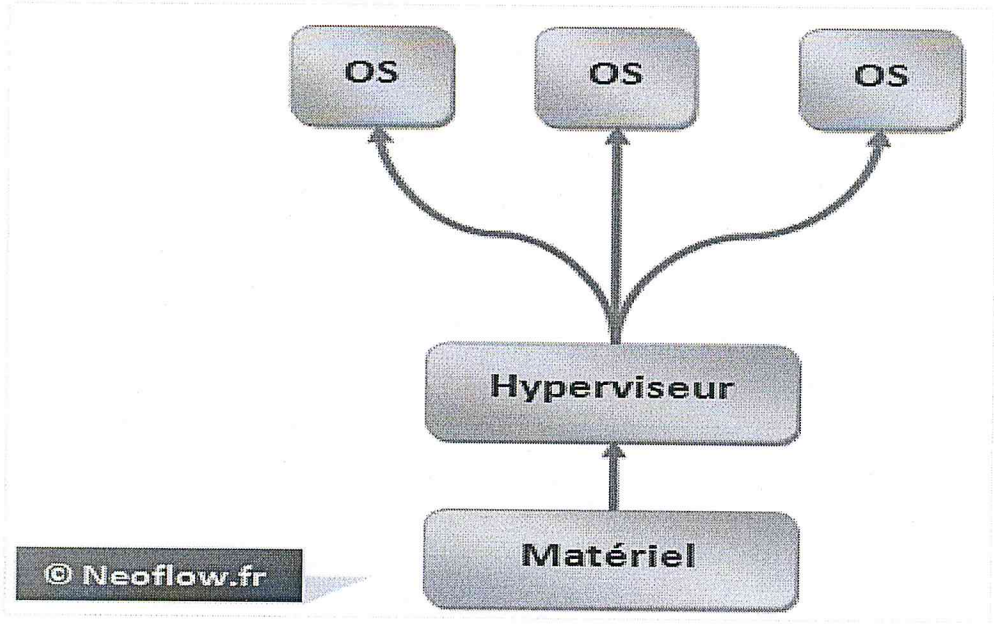


Figure 12 : Hyperviseur de type 1 [25]

b. Hyperviseur de type 2 :

Un hyperviseur de type 2 est un logiciel qui s'installe et s'exécute sur un système d'exploitation déjà en place. De ce fait, plus de ressources sont utilisées étant donné qu'on fait tourner l'hyperviseur et le système d'exploitation qui le supporte, il y a donc moins de ressources disponible pour les machines virtuelles. L'intérêt qu'on peut trouver c'est le fait de pouvoir exécuter plusieurs hyperviseurs simultanément vu qu'ils ne sont pas liés à la couche matérielle.

Parmi les hyperviseurs de type 2, on trouve VMware Player, VMware Workstation, VirtualPC et VirtualBox. [25]

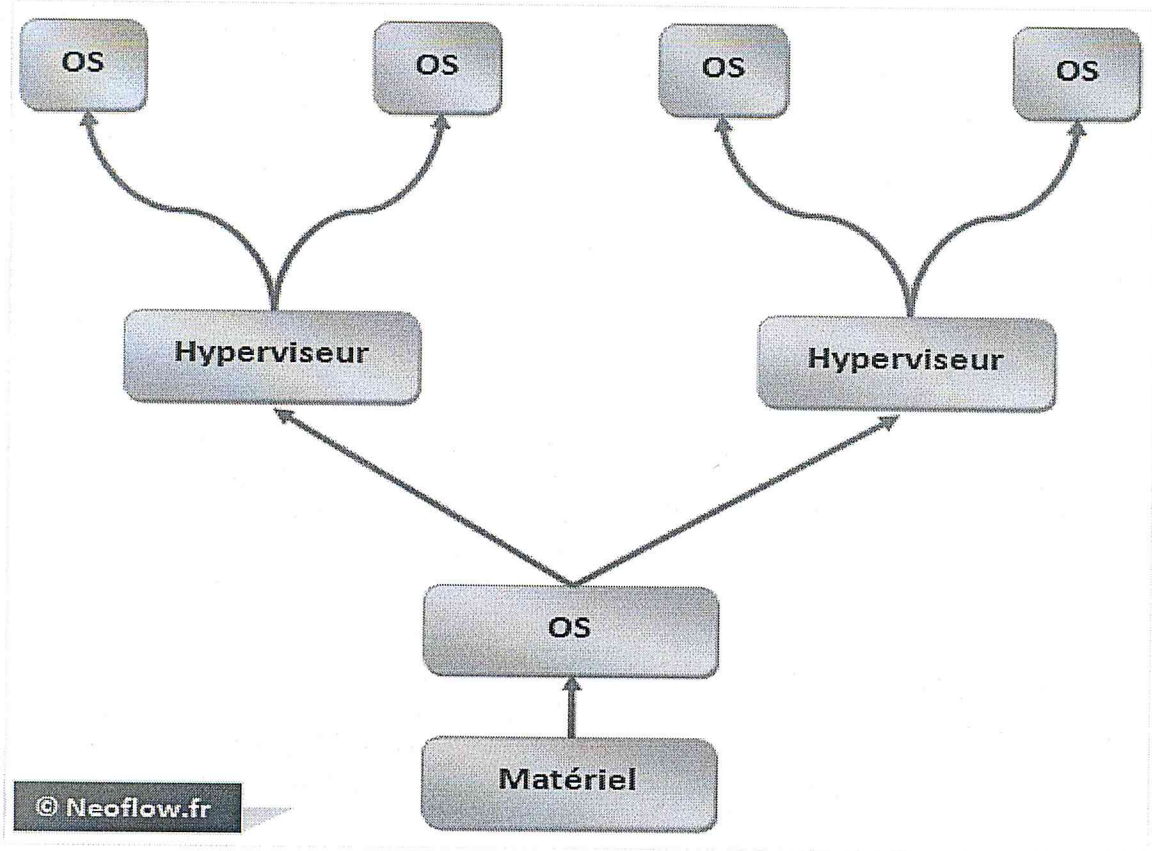


Figure13 : Hyperviseur de type 2 [25]

8.5. Matériel :

Dans ces architectures matérielles, le support de la virtualisation est intégré au processeur ou bien est assisté par ce dernier. Ceci permet de gagner en performances en minimisant la partie logicielle de la virtualisation.

Les exemples les plus connus du marché :

- Hyperviseur IBM Power & Micro-partitionnement AIX
- Mainframes : VM/CMS
- Sun LDOM (hyperviseur pour la gestion de "logical domains")
- Sun E10k/E15k
- HP Superdome
- AMD-V (Assistance à la virtualisation de AMD, anciennement Pacifica)
- Intel VT (Assistance à la virtualisation de Intel, anciennement Vanderpool). [25]

9. La Virtualisation Et le Cloud Computing :

Nous allons montrer les définitions de la virtualisation et le Cloud Computing d'après la conférence du 20 janvier 2009 : Virtualisation, Cloud Computing et SaaS :

C'est à Monsieur **Joseph-Etienne Bernard,** client manager chez Novel de répondre, la virtualisation est un « passe plat » pour faire fonctionner plusieurs systèmes sur un système physique. La définition du Cloud Computing est d'acheter des ressources IT au besoin sans se préoccuper de l'architecture technique. Le Cloud Computing repose sur la virtualisation qui est une technologie.

La parole est à Monsieur **Michel Mestrallet,** Expert en Stratégies Datacenter & Green IT – YIPPEE Consulting. La virtualisation concerne les serveurs, les réseaux, l'infrastructure et le stockage associé à sa sauvegarde. Il convient de fournir un environnement logique indépendant de l'environnement physique. Plusieurs couches de virtualisation sont alors possibles que nous développerons ultérieurement.

Pour **Francis Weill,** Directeur des services managés chez Colt Télécommunications France. La virtualisation c'est découper logiquement une machine physique en n machines physiques. Le Cloud Computing c'est regrouper logiquement des machines physiques en 1 machine logique.

C'est au tour de **Thierry Manfé,** Senior Web technologiste chez Sun Microsystems. Prenons un exemple concret : comment faire tourner un OS sur un autre ? Il est avantageux d'utiliser la Virtual box, un logiciel libre permettant de faire tourner Linux sur Windows et vice versa. Il est donc possible de faire fonctionner plusieurs OS sur une même machine. Les OS ne se voient pas entre eux, ils ont donc le sentiment de tourner sur une machine dédiée. De même, il est possible de virtualiser le stockage et les réseaux. [26]

10. Conclusion :

La virtualisation permet d'assurer une très grande souplesse au niveau des ressources allouables à une solution ou à un client. L'indépendance des solutions matérielles et logicielles permet de donner toute la puissance requise à la bonne exécution du service.

Dans le chapitre suivant on va parler la sécurité.

La sécurité est un en effet un des enjeux primordiaux pour la continuité du développement du Cloud Computing. C'est pourquoi les fournisseurs doivent garantir une sécurisation suffisante des données (intégrité et confidentialité), et assurer la pérennité du service.

Introduction :

L'informatique en nuage est un modèle récent qui tend à résoudre les situations qui nécessitent notamment beaucoup de ressources. Bien que ce modèle soit populaire, l'aspect sécuritaire de l'informatique en nuage peut retarder son adoption massive. En effet, ce type d'architecture se doit de proposer un service fiable en ce qui concerne la disponibilité et la confidentialité des données. Ce type de structure est vraisemblablement sujet à des problèmes de sécurité s'il est confronté à des attaques distribuées.

1. La sécurité en général :

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques. Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information. **[27]**

Rendre vulnérable un système d'information reviendrait à rendre vulnérable l'activité voir la pérennité de l'entreprise. Les compagnies de transport, les banques ou toute autre organisation en dépendent. Ainsi, assurer la sécurité informatique est une priorité vitale. Les menaces contre les systèmes sont nombreuses : destruction, falsification, usurpation des données, ou usage frauduleux d'un réseau. Avec l'avancée d'Internet, la sécurité informatique couvre de nombreux domaines qu'ils soient juridiques, sociaux ou organisationnels.

Concernant les problèmes techniques de la sécurité, on peut distinguer deux catégories :

- La sécurité concernant l'ordinateur proprement dit, système d'exploitation serveur ou poste de travail.
- La sécurité des réseaux. [28]

2. Les principes de la sécurité informatique :

Tout d'abord, il est essentiel de définir les risques et les objets à protéger. Pour cela, on définit un périmètre de sécurité au niveau physique tel que le matériel, les réseaux, les lieux. Mais cette mesure trouve ces limites avec les ordinateurs portables qui peuvent provenir de l'extérieur et s'introduire dans le périmètre de sécurité.

1.1. Pare-feu :

Ces solutions ne sont pas encore suffisantes, il faut empêcher les intrusions venues de l'extérieur. Une technique classique consiste à installer un pare-feu qui va filtrer les communications réseaux. On pourra donc rendre les machines internes invisibles de l'extérieur et réduire certains services ou dialogues réseaux. Pour établir une zone accessible pour les personnes venant de l'extérieur (serveur Web, messagerie ...), il est fréquent d'utiliser une zone démilitarisée (DMZ). [29]

1.2. Sauvegarde des données :

Un autre principe paraissant assez trivial est la sauvegarde des données. En effet, pour chaque type de donnée, on définit une périodicité de sauvegarde en fonction de leur utilisation. On veillera à ce que les supports de sauvegarde soient à l'abri de sinistre ou vers un site externe. On peut alors simuler une panne générale du système d'information qui va pouvoir déceler des failles organisationnelles.

Il existe encore d'autres aspects que nous ne verrons pas ici. Mais nous remarquerons que ces problématiques sont aussi valables dans le domaine matériel que virtuel. [28]

3. Critères fondamentaux de la sécurité informatique :

Les solutions de sécurité qui seront mises en place doivent contribuer à satisfaire les critères suivant :

3.1. la disponibilité :

Pour un utilisateur, la **disponibilité** d'une ressource est la probabilité de pouvoir mener correctement à terme une session de travail. La disponibilité d'une ressource est indissociable de son accessibilité : il ne suffit pas qu'elle soit disponible elle doit être utilisable avec des temps de réponse acceptable. [30]

3.2. L'intégrité :

L'intégrité permet de certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruit tant de façon intentionnelle qu'accidentelle. [31]

3.3. La confidentialité :

La confidentialité est le maintien du secret des informations.

La confidentialité peut être vue comme « la protection des données contre une divulgation non autorisé », il existe deux actions complémentaires permettant d'assurer la

confidentialité des données :

✓ Limiter leur accès par un mécanisme de contrôle d'accès.

✓ Transformer les données par des procédures de chiffrement afin qu'elles deviennent inintelligibles aux personnes ne possèdent pas les moyens de les déchiffrer. [32]

3.4. L'identification et l'authentification :

Un nom associé à des caractéristiques identifie une entité: individus, ordinateur, programme, document, etc. L'identification est la reconnaissance de cette entité.

L'authentification permet de vérifier l'identité annoncée et de s'assurer de la non-usurpation de l'identité d'une entité. Pour cela, l'entité devra produire une information spécifique telle que par exemple un mot de passe (un code, un mot de passe, une empreinte biométrique,...).

L'identification et l'authentification assurent :

✓ **La confidentialité et l'intégrité de données:** seules les entités identifiées et authentifiées peuvent accéder aux ressources et les modifier s'ils sont habilités à le faire.

✓ **La non-répudiation et l'imputabilité :** seules les entités identifiées et authentifiées ont pu réaliser telle action par exemple: preuve de l'origine d'un message ou d'une transaction.

3.5. La non-répudiation :

Est le fait de ne pas pouvoir nier ou rejeter qu'un évènement (action, transaction) a eu lieu. A ce critère de sécurité sont associées les notions d'imputabilité, de traçabilité et éventuellement d'auditabilité.

✓ **L'imputabilité** se définit par l'affectation certaine d'une entité à une action ou un évènement.

✓ **La traçabilité** est la fonction de sécurité qui comprend, l'imputation, mais qui mémorise l'origine d'un message, d'un événement ou d'une donnée. Elle permet par exemple, de retrouver l'adresse à partir de laquelle ces données ont été envoyées.

✓ **L'auditabilité** se définie par la capacité d'un système à garantir la présence des informations nécessaires à une analyse ultérieure d'un évènement (courant ou exceptionnelle) dans le but de déterminer s'il y a effectivement eu violation de la sécurité, et dans ce cas, quelles informations ou autres ressources ont été compromises. [33]

4. La sécurité dans le Cloud :

Gérant une grande quantité de données et de flux, le Cloud est sensible aux problèmes de sécurité. On identifiera les risques et les points cruciaux pour mettre en place une politique de sécurité solide et pérenne.

4.1. Identification des risques de sécurité :

Parmi les risques très connues, Nous commençons avec la perte de maîtrise, c'est-à-dire le transfert de charge des données par l'hébergeur du Cloud, qui fait perdre à l'entreprise le contrôle du système. Ensuite, nous avons le risque de déficiences au niveau des interfaces et des APIs : le cloud étant en émergence, la technologie n'est pas encore mature et a besoin encore d'évolution. Il y a également le risque de conformité et de maintenance de conformité sur l'aspect juridique des données ainsi que sur la traçabilité. On peut parler aussi du risque de la délocalisation des données qui provoque une maîtrise plus faible de celle-ci. Puis, il y a le risque d'isolement des environnements de données sur l'étanchéité entre les différents utilisateurs, l'isolation des données en différentes formes et la monopolisation des ressources par un environnement utilisateur. Enfin nous passons aux derniers risques plus simples : la perte de données, leur récupération, l'usurpation expliquée précédemment et la malveillance dans l'utilisation (par administrateur). [29]

4.2. Sécurité physique :

La dématérialisation des données permet donc d'avoir de multiples Datacenter où peuvent être stockées ces données. Il faut un contrôle et une traçabilité d'accès dans le but de prévenir tout dommage sur le matériel. Faire attention au va-et-vient dans certaines zones, protéger l'accès à certaines salles et même les interdire d'accès peuvent être un bon moyen de protection. Il est impératif de protéger également certaines zones plus que les autres contre les incendies et autres risques environnementaux, ainsi que bien les climatiser.[28]

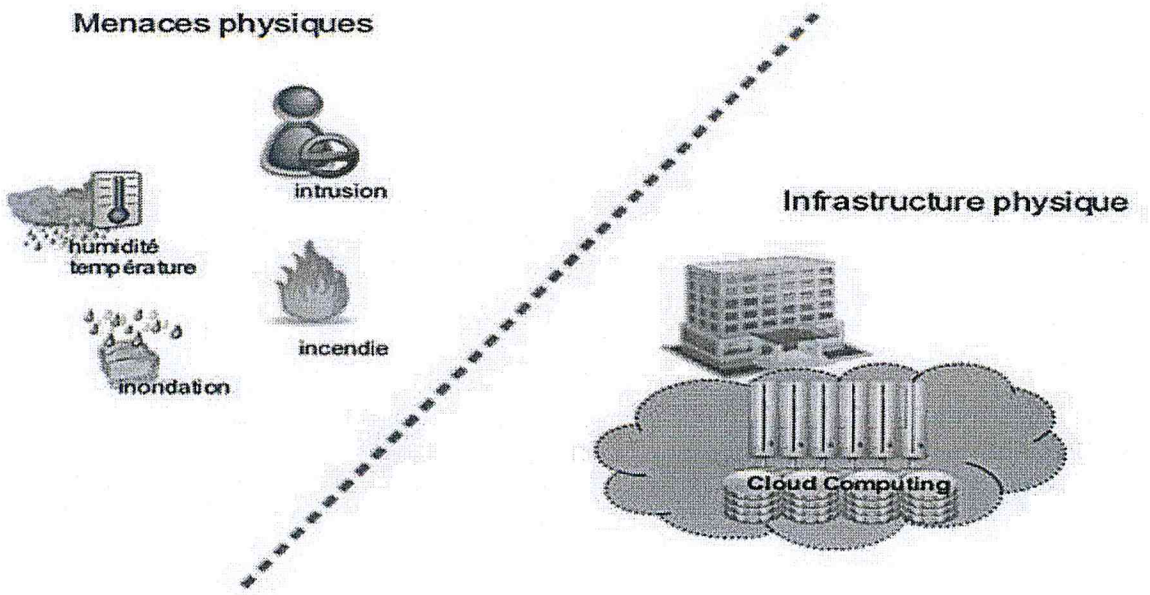


Figure14 : La sécurisation de l'environnement Source [34]

Les redondances matérielles sont également très utilisées pour garantir l'accès au service en très haute disponibilité avec des performances optimales. Penser à la réplication de configuration entre les équipements et également à une redondance avec une sélection d'équipements différents (exemple : constructeur différent) permet de prévenir plusieurs problèmes importants.

Enfin, il est possible de mettre en place comme sécurité géographique, un système de secours géographiquement éloigné, au cas de la perte totale de l'infrastructure. Il permet de réaliser un PCA (plan de continuité d'activité) sans interruption. [28]

4.3. Sécurité logique :

La sécurité que l'on souhaite intégrer est destinée à des plateformes virtualisée. Il faut cependant appliquer les mêmes règles de sécurité que dans une architecture physique. Mais il faut en plus s'intéresser aux problématiques de sécurité spécifiques au Cloud (multi-location). En effet la colocation et le partage de l'infrastructure entre plusieurs utilisateurs imposent des règles strictes de sécurité.

La sécurité et la confidentialité des données peuvent être gérées de différentes façons d'un point de vue logique : la segmentation réseau sera ainsi sécurisée par des équipements de filtrage (pare-feu, proxy, sondes IPS/IDS...) et des solutions antivirus. Le but est ici de contrôler les requêtes entrantes. Un processus d'authentification est par ailleurs nécessaire.

Il faut également insister sur deux bonnes pratiques de sécurisation logique dans un environnement Cloud. Tout d'abord, il faut paramétrer le système d'exploitation des machines virtuelles pour les sécuriser comme le conçoit l'éditeur de la solution de virtualisation. La deuxième bonne pratique consiste à bien isoler le trafic réseau en fonction des besoins lors de la conception du réseau virtuel. [29]

4.4. Sécurité des données :

Pour la sécurité des données, on peut naturellement se diriger vers des solutions de chiffrement. Notamment la méthode classique consistant à créer un couple clé publique/clé privée où seul le destinataire est en mesure de déchiffrer les données qui lui sont destinées grâce à sa clé privée. Il est important de mentionner que même le fournisseur de cloud ne détiendra pas la clé privée. Cette solution permet de bien sécuriser les données (selon la taille de la clé) et le client à la possibilité de ne chiffrer qu'une partie de ses données. La méthode pose cependant certaines problématiques d'implémentation. Lors de certains traitements tels que la sauvegarde ou l'indexation, il peut s'avérer nécessaire de manipuler des données décryptées. [29]

5. Les attaques :

5.1. Définition d'une attaque :

Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables. [35]

5.2. Définition d'un Pirate (Hacker) :

Un pirate est une personne qui va rechercher des failles afin d'optimiser un système. Le dit-système peut être un ordinateur, un site, une architecture réseau ou même un téléphone portable. Le but n'est pas de détruire, le but est de construire. Pourtant tous les Etats ne comprennent pas ce terme de la même manière. [36]

5.3. Buts d'attaques :

5.3.1. Interruption : vise la **disponibilité** des informations (DoS, . . .).

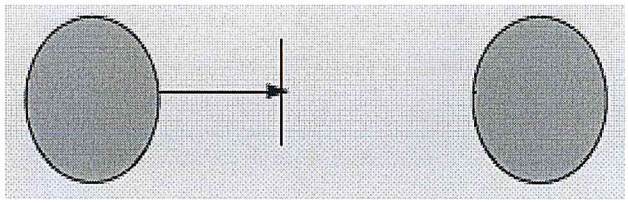


Figure 15 : attaque par Interruption [37]

5.3.2. Interception : vise la **confidentialité** des informations (capture de contenu, analyse de trafics...).

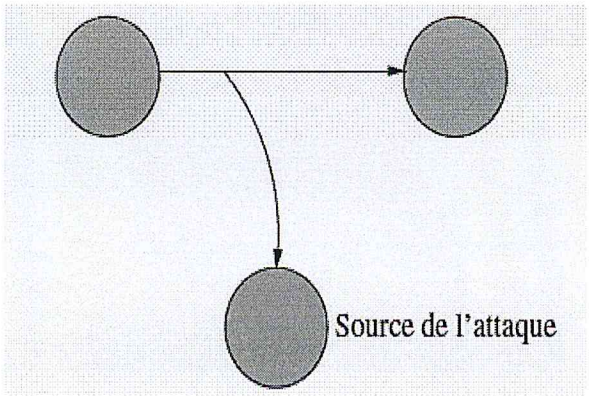


Figure 16 : attaque par Interception [37]

5.3.3. Modification : vise **l'intégrité** des informations (modification, rejeu,. . .).

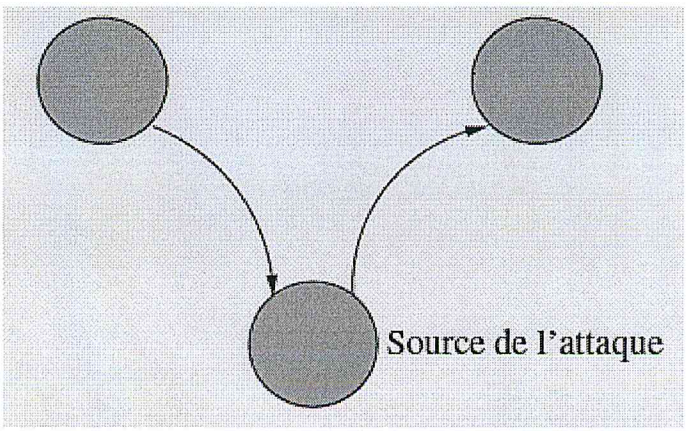


Figure 17 : attaque par Modification [37]

5.3.4. Fabrication : vise l'authenticité des informations (mascarade, . . .).

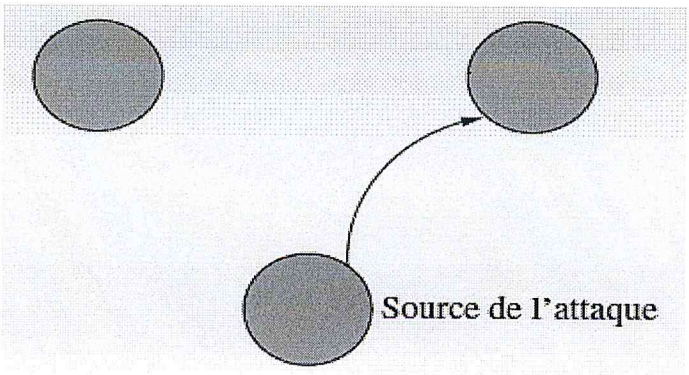


Figure 18 : attaque par Fabrication [37]

5.4. Les types d'attaques usuels :

Parmi les différents problèmes de sécurité réseau, on peut recenser quatre types d'attaques qui peuvent affaiblir un système d'information : les attaques d'accès, de modification, de déni de service et de répudiation.

5.4.1. Attaques d'accès :

Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information.

a. Le sniffing :

Cette attaque est utilisée par les pirates informatiques pour obtenir des mots de passe. Grâce à un logiciel appelé renifleur de paquets (sniffer), on peut intercepter toutes les paquets qui circulent sur un réseau même ceux qui ne nous sont pas destinés. Par exemple, lors d'une connexion grâce à « telnet » le mot de passe de l'utilisateur va transiter en clair sur le réseau. Il est aussi possible de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Cette technologie n'est pas forcement illégale car elle permet aussi de détecter des failles sur un système.

b. Les chevaux de Troie :

Les chevaux de Troie sont des programmes informatiques cachés dans d'autres programmes.

Ce nom vient de la légende grecque de la prise de Troie à l'aide d'un cheval en bois rempli de soldats qui attaquèrent la ville une fois à l'intérieur.

En général, le but d'un cheval de Troie est de créer une porte dérobée (backdoor) pour qu'un pirate informatique puisse ensuite accéder facilement l'ordinateur ou le réseau informatique. Il peut aussi voler des mots de passe, copier des données, exécuter des actions nuisibles.

c. Porte dérobée :

Lorsqu'un pirate informatique arrive à accéder à un serveur à l'aide d'une des techniques présentées dans cette section, il souhaiterait y retourner sans avoir à tout recommencer. Pour cela, il laisse donc des portes dérobées (backdoor) qui lui permettra de reprendre facilement le contrôle du système informatique.

Il existe différents types de portes dérobées :

- Création d'un nouveau compte administrateur avec un mot de passe choisi par le pirate.
- Création de compte ftp .
- Modification des règles du pare-feu pour qu'il accepte des connections externes.

Dans tous les cas, l'administrateur perte le contrôle total du système informatique. Le pirate peut alors récupérer les données qu'il souhaite, voler des mots de passe ou même détruire des données.

d. L'ingénierie sociale :

L'ingénierie sociale (social engineering en anglais) n'est pas vraiment une attaque informatique, c'est plutôt une méthode pour obtenir des informations sur un système ou des mots de passe. Elle consiste surtout à se faire passer pour quelqu'un que l'on n'est pas (en général un des administrateurs du serveur que l'on veut pirater) et de demander des informations personnelles (login, mots de passe, accès, numéros, données...) en inventant un quelconque motif (plantage du réseau, modification de celui-ci...). Elle se fait soit au moyen d'une simple communication téléphonique ou par courriel.

e. Le craquage de mots de passe :

Le craquage consiste à faire de nombreux essais jusqu'à trouver le bon mot de passe.

Il existe deux grandes méthodes :

- L'utilisation de dictionnaires : le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci (à l'envers, avec un chiffre à la fin...). Les dictionnaires actuels contiennent dans les 50 000 mots et sont capables de faire une grande partie des variantes.

• La méthode brute : toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution.

5.4.2. Les attaques de modification :

Une attaque de type « modification » consiste, pour un attaquant à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information.

Virus, vers et chevaux de Troie :

Il existe une grande variété de virus. On peut cependant définir un virus comme un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs.

Les dégâts causés vont du simple programme qui affiche un message à l'écran au programme qui formate le disque dur après s'être multiplié. On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication :

- Les vers capables de se propager dans le réseau;
- Les « chevaux de Troie » créant des failles dans un système;
- Les bombes logiques se lançant suite à un événement du système;
- Les canulars envoyés par mail.

5.4.3. Les attaques par saturation (déni de service) :

Les attaques par saturation sont des attaques informatiques qui consistent à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes.

Cette technique de piratage assez simple à réaliser est jugée comme de la pure malveillance. Elle ne fait que bloquer l'accès aux sites, sans en altérer le contenu.

Il existe différente attaque par saturation :

- Le flooding
- Le TCP-SYN flooding
- Le smurf
- Le débordement de tampon

(Pour plus de détailler voir le quatrième chapitre).

5.4.4. Les attaques de répudiation :

La répudiation est une attaque contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passé.

L'IP spoofing :

Cette attaque consiste à se faire passer pour une autre machine en falsifiant son adresse IP. Elle est en fait assez complexe. Il existe des variantes car on peut spoofer aussi des adresses e-mail, des serveurs DNS ou NFS. [38]

6. Les outils de la sécurité :

6.1. Antivirus :

Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants (malwares en anglais), également appelés virus,Chevaux_de_Troie ou vers selon les formes. **http://www.futura-sciences.com**

6.2. système de détection les intrusions (IDS) :

On appelle **IDS** (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

Il existe deux grandes familles distinctes d'IDS :

- Les **N-IDS** (Network Based Intrusion Detection System), ils assurent la sécurité au niveau du réseau.
- Les **H-IDS** (Host Based Intrusion Detection System), ils assurent la sécurité au niveau des hôtes.

6.3. Pare-feu (Firewall) :

Un firewall (ou pare-feu) est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).

Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

6.4. Biométrie :

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. D'autre part, comme nous allons le voir, les caractéristiques physiques sont loin d'être si parfaites et si précises, et l'on atteint très vite des limites pour ces techniques. Par exemple : empreintes digitales. [41]

6.5. Réseau virtuel privé « VPN » :

Un réseau privé virtuel (Virtual Private Network en anglais) est une terminologie qui regroupe plusieurs technologies visant à isoler des réseaux de façon logique tout en leur faisant partager la même infrastructure physique. Ces technologies sont massivement utilisées, notamment par les opérateurs, pour réduire les coûts d'installation des infrastructures. [42]

6.6. Cryptographie :

La cryptographie quantique n'est pas un algorithme de chiffrement à proprement parler : elle permet simplement de mettre en œuvre un algorithme de cryptographie classique, et même ancien, qui est le seul démontré sans failles : le "masque jetable". Cet algorithme, bien que parfaitement sûr, est peu utilisé car il nécessite un échange de clé de longueur aussi grande que le message à transmettre. Cet échange de clé pose des problèmes de sécurité aussi importants que la transmission du message en lui-même, ce qui limite le domaine d'applicabilité de cet algorithme. [43]

La cryptographie est donc un ensemble des techniques permettant de protéger une communication au moyen d'un code graphique secret. [44]

permet d'assurer les fonctions principales de la sécurité des systèmes d'informations : la détection de la perte de l'intégrités, l'identification des interlocuteurs, l'authentification et la non-répudiation des messages, et la confidentialité des informations. [45]

Conclusion :

Nous avons vu dans ce chapitre les différentes notations de sécurité ainsi les différents types d'attaque existants, et la stratégie de sécurité utilisée par une entreprise pour protéger ces ressources et assurer les services de la sécurité (l'intégrité, disponibilité, confidentialité). Mais malgré toutes ces planifications, le système reste exposer aux attaques, et le taux de risque existe toujours, donc il n'est possible de mener une stratégie de sécurité ou la vulnérabilité et le risque sont nuls.

C'est pour ça il faut toujours rester au courant des nouveaux attaques et des nouveaux outils et mécanismes concernant la technologie de sécurité, et surtout la définition des réactions en cas d'une menace.

Introduction :

De nos jours les réseaux informatiques sont de plus en plus présents dans les milieux professionnels ainsi que chez les particuliers. Ces dix dernières années ont vu l'avènement de l'internet, et son apparition dans la plupart des foyers, du moins dans les pays développés. Cette évolution a favorisée la communication, l'expansion du commerce, l'accès à l'information et de nombreuses sociétés dépendent maintenant entièrement de leur réseaux. Les particuliers utilisent de plus en plus l'internet pour échanger des données sensibles telles que des informations de paiement en ligne.

Toutes ces innovations ont permis de faciliter la vie de tous à chacun mais ont aussi contribué au développement de nouveaux risques que sont les attaques informatiques. Les méthodes de piratages sont de plus en plus nombreuses et perfectionnées, elles peuvent se traduire par des vols d'informations cadentielles, des destructions de données numériques, des coupures de services voire même des dégâts matériels. Nous nous intéresserons ici à un type d'attaque assez répandu: le Déni de Service ou Dos. Cette attaque bien que peu dangereuse pour l'intégrité des données peut s'avérer très pénalisante pour une société car elle vise à rendre indisponible une ressource réseau. Ainsi une société de e-commerce ne peut se permettre de perdre son site internet même pour quelques minutes car elle perdrait des milliers voire des millions d'euros.

Nous allons tout d'abord définir les attaques dos, pour mieux comprendre d'où elles proviennent, comment elles sont exécutées et quelles en sont les principales conséquences. Nous verrons ensuite comment détecter et contrer de telles attaques dans un réseau en se penchant sur l'efficacité des solutions existantes. Puis nous tenterons de proposer une solution adaptée pour les détecter.

1. Définition :

Le déni de service, connu sous le titre anglophone de "Denial Of Service" ou encore DOS, est une attaque réalisée dans le but de rendre indisponible durant une certaine période les services ou ressources d'une organisation. Généralement, ce type d'attaque à lieu contre des machines, serveurs et accès d'une entreprise afin qu'ils deviennent inaccessibles pour leurs clients. Le but d'une telle attaque n'est pas d'altérer ou de supprimer des données, ni même de voler quelconque information. Il s'agit ici de nuire à la

réputation de sociétés présentes sur Internet en empêchant le bon fonctionnement de leurs activités. [46]

2. Historique des grandes attaques DOS :

- Nuke en avril 1992 (Icmp_unreach)
- Octopus en janvier 1996 (While – connect)
- Ping Of Death en décembre 1996
- Smurf en juillet 1997
- Land en octobre 1997 (Windows 95, NT 4.O et 98)
- Latierra en octobre 1997 (Plante Windows 95 et occupe 100% du CPU sur NT 4.0)
- Teardrop / Overdrop en décembre 1997 (Plante Linux, NT et 95)
- Syndrop en juin 1998 (Teardrop en tcp avec le bit syn et des champs invalides)
- Snork en septembre 1998 (Tueur de Windows NT, envoi de paquet RPC (135/UDP) de la part d'un autre NT)
- Smack en octobre 1998 (Inondation de paquets ICMP-UNREACHABLE aléatoires)
- Attaque sur le serveur de mise à jour de Microsoft
- Attaque de sites Web connus tels que Google, Microsoft, Apple Computer ...
- Attaques de type « ping flood » en octobre 2002 sur les serveurs racines DNS...

3. Les techniques d'attaques :

Les techniques d'attaque : Les attaquants utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes :

- Les attaques directes.
- Les attaques indirectes par rebond.
- Les attaques indirectes par réponses.

Nous allons voir en détail ces trois familles.

3.1. Les attaques directes :

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. La plupart des "script kiddies" utilise cette technique. En effet, les

programmes de hack qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime. [47]

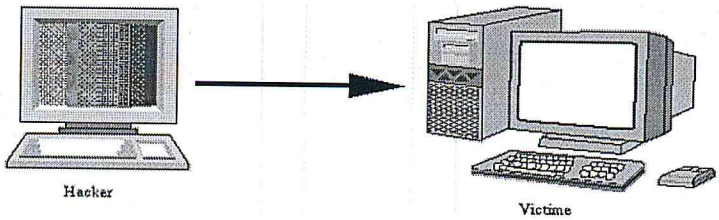


Figure19 : Attaque directe [47]

Si nous nous faites attaqués de la sorte, il y a de grandes chances pour que nous puissions remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant. Depuis quelques ans, on n'utilise jamais cette technique car il n'est pas efficace quand on utilise une machine normale pour attaquer un serveur très performant. [47]

3.2. Les attaques indirectes par rebond :

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) du hacker.
- Eventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...) pour attaquer. Le principe en lui-même, est simple: Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond. [47]

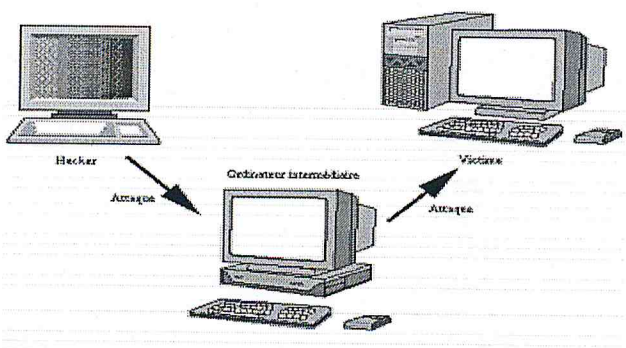


Figure 20 : Attaque indirect par rebond. [47]

L'attaque FTP Bounce fait partie de cette famille d'attaque. Si nous sommes victime de ce genre d'attaque, il n'est pas facile de remonter à la source. Au plus simple, nous remontrons à l'ordinateur intermédiaire. [47]

3.3. Les attaques indirectes par réponse :

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime. [47]

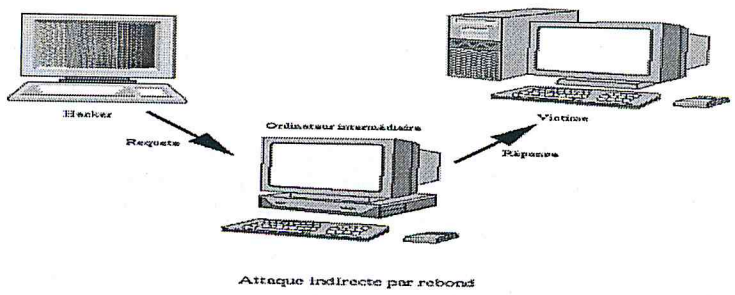


Figure 21 : Attaque indirecte par reponse. [47]

4. Les conséquences :

Une attaque par Dos peut avoir de nombreuses formes qui engendrent chacune de nombreuses Conséquences, représentant une palette de risques très variées. Les attaques les plus dévastatrices peuvent amener, que ce soit de manière directe ou indirecte, à des pertes d'argents colossales pour une société dont la principale activité est basée sur un flux d'informations Internet. Dans un monde où un grand nombre des entreprises utilisent leurs sites internet comme leur principale vitrine, et où leur chiffre d'affaires dépend de ce même site, les attaques contres celui-ci peuvent amener à des pertes d'argent colossales.

Une attaque par déni de service étant, le plus souvent temporaire, les auteurs utilisent allégrement le chantage pour extorquer des fonds aux entreprises. Il est clair que pour une société d'e-commerce par exemple, un blocage de son site pourrait lui faire perdre plusieurs millions par heure. Payer les auteurs peut donc parfois s'avérer être une solution beaucoup moins couteuse, même si cela signé céder au chantage, et que rien ne garantit que l'auteur de l'attaque ne récidivera pas. On remarque, au _l des années, que ce genre de pratique est

de plus en plus utilisé dans le monde du cyber-terrorisme, puisque ces attaques sont relativement simples à mettre en place, et que toutes les sociétés dépendantes d'internet sont menacées. [48]

5. Les différentes attaques dos :

Les attaques DoS prennent de multiple formes et utilisent de nombreuse méthodes différentes pour mettre hors service une ressource réseau, nous allons essayer de définir ici de manière none xhaustive les différentes attaques connues et répandues.

5.1. Les attaques par surcharge :

Une des méthode les plus répandue et une des plus simple a mettre en œuvre est de surcharger complètement la cible de requêtes de toutes sortes. On distingue quatre grands types d'attaques utilisant différents protocoles et couches réseaux. [48]

- **Le SynFlooding :**

Parmi les attaques précédemment citées, nous nous sommes principalement focaliser sur les attaques de type Syn Flood pour saturer un service en l'inondant de requêtes. Sa mise en œuvre a requis l'utilisation d'attaques sous-jacentes comme l'IP-Spoofing, PING-Flood.

Le principe est de laisser sur la machine cible un nombre important de connexions TCP en attentes. Pour cela, le pirate envoie un très grand nombre de demandes de connexion (flag SYN à 1). La machine cible renvoie alors les SYN-ACK en réponse au SYN reçus. Le pirate ne répondra jamais avec un ACK, et donc pour chaque SYN reçu, la cible aura une connexion TCP en attente dans une file d'attente ou queue de message. Etant donné que ces connexions semi-ouvertes consomment des ressources mémoires, au bout d'un certain temps, la machine est saturée et ne peut plus accepter de nouvelle connexion. Ce type de déni de service n'affecte que la machine cible.

Le pirate emploie généralement l'IP Spoofing (création de paquet IP avec une adresse source falsifiée) afin de masquer son identité. Cependant, puisqu'il usurpe l'identité d'une autre machine, il lui faudra s'assurer que celle-ci ne répondra pas aux SYN-ACK émis par la victime (on entend par "réponse" une requête de type RESET précisant que le SYN-ACK reçu n'était pas attendu).

Les machines vulnérables aux attaques SYN mettent en file d'attente, dans une structure de données en mémoire, les connexions ainsi ouvertes, et attendent de recevoir

un paquet ACK. Il existe un mécanisme d'expiration permettant de rejeter les paquets au bout d'un certain délai. Néanmoins, avec un nombre de paquets SYN très important, si les ressources utilisées par la machine ciblent pour stocker les requêtes en attente sont épuisées, elle entre dans un état où elle ne peut fournir le service. [49]

Le principe de fonctionnement d'une connexion TCP :

Normalement, lorsqu'une connexion TCP est initialisée entre le serveur et un client sans la moindre intention de nuire, un échange de message doit avoir lieu. Selon le principe du *« three-wayhandshake »*, la connexion doit se dérouler en trois phases notamment : le SYN, le SYN-ACK et l'ACK. Le client qui souhaite se connecter avec le serveur doit d'abord, en effet, envoyer un premier paquet de SYN (Synchronized) au serveur. Ensuite pour répondre à cette requête, le serveur lui envoie un message SYN-ACK (SynchronizedAcknowledgment), et le client doit enfin envoyer une réponse ACK (Acknowledgment) pour établir définitivement la connexion. [50]

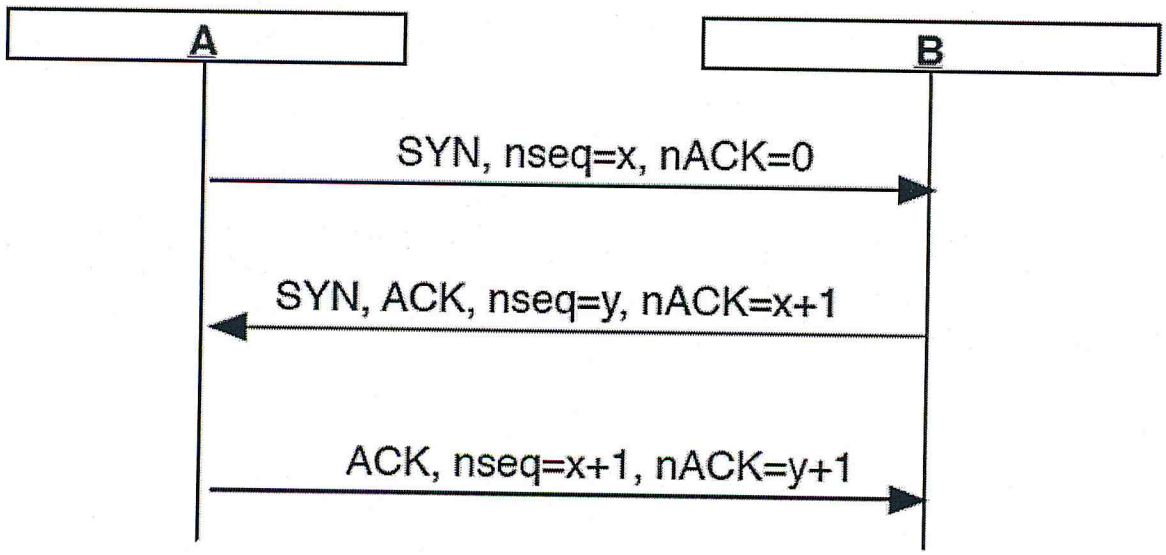


Figure22 : Ouverture d'une connexion en TCP [51]

Remarque :

- Les numéros de séquence initiaux x et y sont choisis "aléatoirement".
- Un timer est déclanché après l'envoi d'un SYN.
- Si une réponse tarde trop à arriver (>75s), la connexion est abandonnée.

Se protéger :

- une bonne configuration des firewalls permet de détecter/limiter ce type d'attaque. Par exemple, on peut limiter le nombre de connexions TCP par seconde. [51]

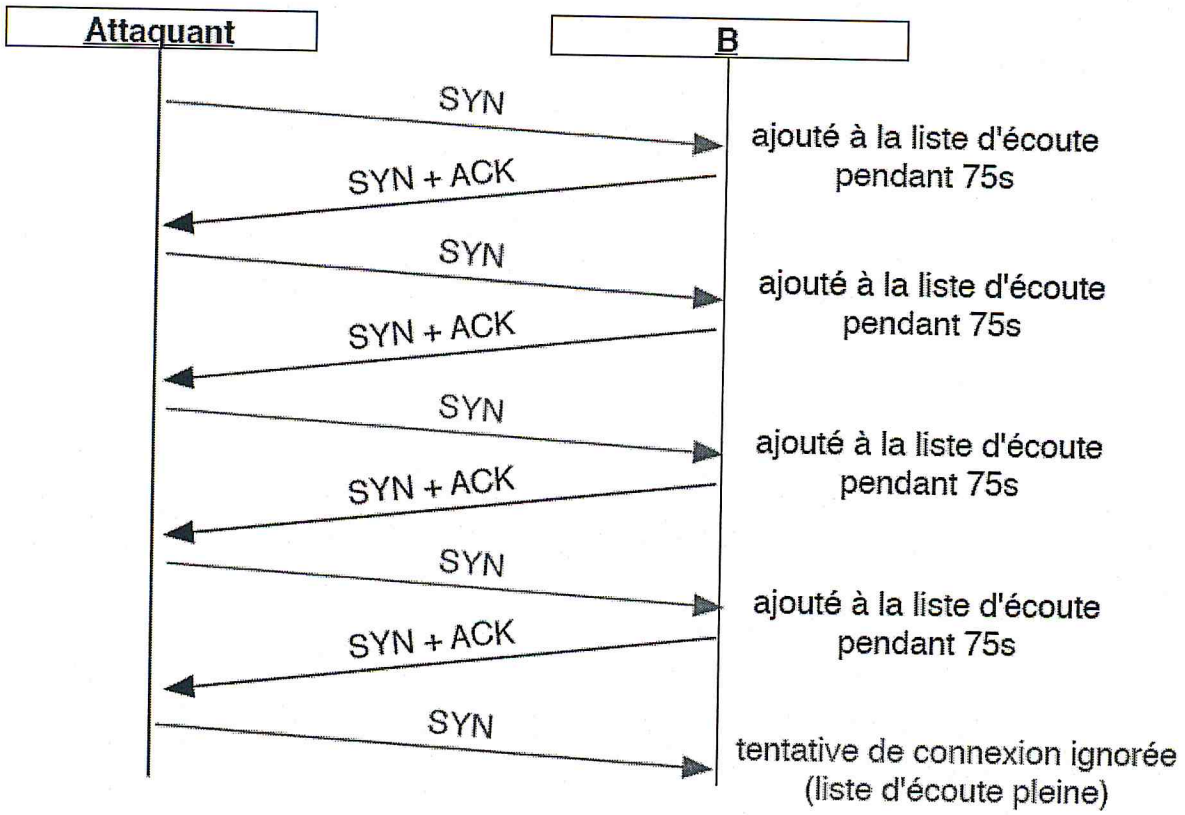


Figure 23 : Attaque SYN Flood [51]

5.2. Les attaques par failles :

Un autre moyen de réaliser un DoS consiste à exploiter les nombreuses failles présentes dansles systèmes d'informations. Au lieu de chercher à surcharger la cible, on va simplement laforcer à réagir de façon bien définit en lui soumettant des informations qu'elle ne peut gérer. Les systèmes Microsoft Windows sont par exemple très vulnérables à ce genre d'attaques. [48]

Comme par exemple :

- **Le Ping de la mort :**

Un ping a normalement une longueur maximale de 65535 ((2 exp 16) - 1) octets, incluant une entête de 20 octets. Un ping de la mort c'est un ping qui a une longueur de données supérieure à la taille maximale. Lors de son envoi, le ping de la mort est fragmentée en paquets plus petits. L'ordinateur victime qui reçoit ces paquets doit alors les

reconstruiront. Certains systèmes ne gèrent pas cette fragmentation, et se bloquent, ou crashent complètement. D'où le nom de cette attaque.

Pour le protégé on fait les mises à jour des systèmes d'exploitation, et effectuer un test avant que quelqu'un d'autre le fasse à votre place. Si le système réagi correctement, il n'y a pas de problème. [41]

5.3. Les attaques distribuées :

La plupart des attaques, cité plus haut, peuvent être exécutés de manière distribuée, on parle alors de DDoS pour Distributed Denial of Service. Les attaques distribuées se basent sur ce fait : attaquer une cible toute seule se traduit souvent par un échec, alors que si un grand nombre de machines s'attaquent à la même cible alors l'attaque a plus de chance de réussir. [48]

Ce sont actuellement les attaques les plus dévastatrices. Elles reposent sur l'utilisation d'agents aussi appelés daemons qui sont déployés sur lemaximum de machines possible. Le pirate installe le daemon3 sur dès ma chines mal sécurisées connectées a- internet, soit en les piratant, soit à l'aide d'un ver. Les agents exécuteront alors simultanément les commandes ordonnées par le pirate pour attaquer une cible prédéfinie. [52]

5.4. Les attaques par usurpation :

La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu). En effet, un système pare-feu (en anglais *firewall*) fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines internes au réseau.

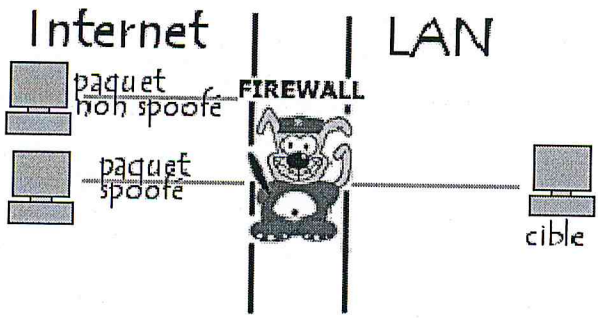


Figure 24: attaques par usurpation [35]

Ainsi, un paquet spoofé avec l'adresse IP d'une machine interne semblera provenir du réseau interne et sera relayé à la machine cible, tandis qu'un paquet contenant une adresse IP externe sera automatiquement rejeté par le pare-feu. Cependant, le protocole TCP (protocole assurant principalement le transport fiable de données sur Internet) repose sur des liens d'authentification et d'approbation entre les machines d'un réseau, ce qui signifie que pour accepter le paquet, le destinataire doit auparavant accuser réception auprès de l'émetteur, ce dernier devant à nouveau accuser réception de l'accusé de réception. [35]

6. Les outils d'attaques :

Il existe de nombreux outils servant _a perpétrer des dénis de services selon le système, quel'on soit sous Windows, Linux ou autres systèmes d'exploitations. Linux reste quand même le système comportant le plus d'outils dont nous détaillerons quelques fonctions.

6.1. HPing :

Est avant tout un outil de manipulation de paquet qui fonctionne à la manière duping, mais qui n'y est pas limité. En effet, il peut utiliser d'autres protocoles dont TCP etUDP, d'ailleurs, par défaut, il tourne en mode TCP. Cependant, ses fonctionnalités peuvent également servir à tester la sécurité du réseau et de ses équipements.

Cet outil nous vante d'ailleurs des mérites très alléchants :

- Tester les règles de firewall
- Réaliser des scans de port avancés
- Tester les performances réseau en utilisant différents protocoles, tailles de paquet, TOS (type of service) et la fragmentation
- Découverte des chemins MTU
- Transférer des données à travers et malgré le durcissement de politique des firewall
- Tracerouter via divers protocoles,
- Faire du Firewalk
- Fingerprinter l'OS des machines distantes
- Auditer la stack TCP/IP
- et plein d'autres choses. [54]

Quelque commande utile :

- hping 192.168.0.1 -1 : le ping classique.
- hping 192.168.0.1 -a 192.168.0.11 : l'option -a définit l'adresse source du ping et donc l'adresse qui recevra les réponses en provenance de la cible.
- hping 192.168.0.1 -i u10 : pour envoyer 1 paquet toutes les 10 s'avérer. [48]

6.2. Dsniff :

Dsniff est à la fois une suite d'utilitaire et un utilitaire lui-même d'audit réseau permettant aisément de sniffer les mots de passe circulants en clair, dans des protocoles non sécurisés. Afin de ne pas nous perdre dans les différents programmes de sa suite, nous les regrouperons sur cette page. Ainsi, Il détecte automatiquement les protocoles d'application, en capturant seulement les données intéressantes (Des mots clefs : pass, user,...).

Quelques Exemples d'utilisation :

- Pour capturer tous les logins/pass circulant à travers sa carte réseau (notre interface réseau est *eth0*) : bt ~ # dsniff -i eth0.
- Pour les enregistrer dans un fichier : bt ~ # dsniff -i eth0 -w pass.txt.
- Pour capturer tous les logins/pass du service ftp : bt ~ # dsniff -i eth0 -f ftp. [55]

7. Les moyens de se prémunir :

Comme on a pu le voir dans la partie précédente, il est très important de se prémunir contre ces attaques faciles à réaliser et pouvant provoquer de graves dégâts. Le problème est qu'il est très dur de les détecter encaquement, car elles ne sont pas évidentes à différencier des autres attaques. En été, il faut réussir à différencier un grand nombre de connexions légitimes d'une attaque afin de détecter le minimum possible de faux positives tout en ne laissant passer aucunes attaques ! Parfois, un déni de service peut même résulter de la popularité soudaine d'un site web sans qu'il y soit d'attaquant mal intentionné, dans ce cas comment proposer une méthode de détection efficace dans toutes les situations. Il existe plusieurs moyens, plus ou moins efficace, permettant de détecter et/ou de bloquer ces attaques.

7.1. Les mises à jour systèmes :

La première chose à faire, pour éviter les dénis de services applicatifs, est de maintenir tous les logiciels de son système à jour puisque les mises à jours permettent souvent de corriger des failles logicielles, qui peuvent être utilisées par un attaquant, pour mettre l'application (Par exemple un serveur web) hors service, ou pire, le serveur. Il est donc impératif de mettre son système à jour très régulièrement C'est un moyen très simple à mettre en place pour se protéger des attaques applicative, mais les administrateurs effectuent souvent ces mise à jour irrégulièrement. Une autre chose sur laquelle il faut porter l'attention : la configuration de ces serveurs. Une mauvaise configuration de ces serveurs peut donner accès à des fichiers importants.

Mais cette fois-ci, il est beaucoup plus dur de mettre en place une configuration bien sécurisée car il faut penser à beaucoup de choses. De plus, lorsque qu'on exécute une modification sur son serveur, il faut penser si celle-ci n'a pas d'impact sur les autres services, et donc sur la sécurité du serveur.

7.2. IDS/IPS :

Les IDS sont chargés de distinguer les activités normales des activités parasites et/ou malveillantes. Il existe deux catégories d'événements que les IDS doivent analyser:

- **anomalie intrusion détection :** Il s'agit de la détection des comportements inhabituels de certains utilisateurs. Ce type de détection peut toutefois engendrer des fausses alertes, un comportement inhabituel n'étant pas forcément malveillant ou dangereux;
- **mésuse intrusion détection :** C'est la détection du mauvais fonctionnement d'un système informatique. La détection est basée sur des modèles prédéfinis d'attaques (signatures) qui exploitent les failles d'un système. Cette détection protège très bien contre les attaques connues, analysées et définies dans les modèles implémentés, mais ne réagit pas aux nouvelles attaques puisque leur signature n'est pas encore connue. Il faudra donc prévoir d'apprendre à l'IDS ces nouvelles signatures.

En fonction de leur réactivité aux attaques, les IDS se classent en:

- **IDS passifs:** ils génèrent simplement des alarmes en cas d'attaques (enregistrées dans un fichier de logs, envoyées par mail, par SMS, etc.);
- **IDS actifs:** ils génèrent les alarmes, mais en plus déclenchent un processus de défense contre l'attaque.

Les IDS actifs ont ainsi évolué vers les produits IDP/IPS (Intrusion Détection and Prévention/Intrusion Prévention System). Toutefois, ils ne sont pas aisés à utiliser car ils peuvent générer beaucoup de fausses alertes.

La valeur des produits IDP/IPS réside dans leur capacité à bloquer immédiatement les attaques détectées! Un bon produit IDP/IPS, même s'il ne sera jamais parfait, devra:

- ne pas bloquer ou perturber le fonctionnement normal d'une entreprise ou d'une administration;
- réagir immédiatement et bloquer l'attaque constatée,
- agir complémentairement au firewall,
- utiliser plusieurs algorithmes de lutte contre les attaques,
- faire la différence entre un événement normal et un évènement provoqué pour éviter les fausses alertes. [56]

Les IPS Les IPS (Intrusion Prévention System) sont, aux différences des IDS, un ensemble de matériel et de logiciel ayant pour but d'empêcher les intrusions ou autres activités suspectes détectés. Les IPS sont donc des outils actifs permettant de stopper toutes activités suspectes, contrairement aux IDS qui ne font que les détecter. [48]

7.3. Le Pare-feu (Firewall) :

Les firewalls sont des équipements réseaux qui permettent de filtrer les paquets entrants et sortants afin de prévenir toutes attaques de l'extérieur. Ils se basent sur un fonctionnement séquentiels et un ensemble de règles pour autoriser seulement les connexions légitimes. Dans le cadre des DoS, le problème majeur est que les attaquants utilisent des connexions légitimes pour perpétrer leurs attaques. De plus, les firewalls ne peuvent pas efficacement différencier les connexions légitimes et illégitimes. Par contre ils peuvent se révéler très efficace pour contrer un attaquant. En se basant sur les informations

fournit par des équipements de détections, on peut appliquer des règles très précises qui bloqueront uniquement les connexions malfaisantes, en se basant sur le protocole, l'IP ou le port.

De nombreux firewalls hardware ou software permettent de se prémunir contre les attaquants.

Parmi eux, un des plus courants est le firewall intégré au noyau Linux : Netfilter et son interface iptables. Il présente l'avantage d'être open source donc gratuit et d'être assez facile à appréhender. De plus, cela n'a aucune influence sur sa puissance et sa modularité.

Bien maitriser un firewall peut être une très bonne protection contre la majorité des attaques et des attaquants. Il est nécessaire de surveiller les connexions qui transitent sur son réseau pour être capable de bien se protéger contre toutes menaces. [48]

8. Conclusion:

Les attaques par déni de services existent depuis de nombreuses années et sont parfois médiatisés. Elles ont su se développés au fur et à mesure du développement des systèmes informatiques, tout en étant simple à mettre en œuvre. Bien qu'aujourd'hui, il existe des outils de détections et de protection contre le déni de service, ils sont toujours complexes à mettre en place avec une efficacité pas toujours optimale. Avoir une multitude d'outil ne suffit pas, il faut surtout être réactif lorsque l'on subit une attaque, mais aussi avoir une bonne politique de sécurité, non pas pour supprimer totalement les risques, car le risque zéro n'existe pas, mais au moins limiter l'impact d'une attaque de type déni de service face au service que l'on protège. Mais aujourd'hui, les pirates ont accès à des ressources de plus en plus importantes, leurs attaques sont donc de plus en plus difficiles à contrer. La lutte contre les pirates n'est donc pas prête de s'arrêter.

1. Introduction :

Malgré que le domaine de la virtualisation n'est pas un nouveau domaine mais son utilisation dans les applications est augumenté ces dernières années par exemple dans les centres de données (data centers) et le cloud. Par conséquant, le besoin de sécuriser la virtualisation et ces infrastructrures (Machines virtuelles ,hyerviseur,...)est devenu très necesssiare et important parce que la virtualisation est menacée par pleusieurs types d'attaques parmi les attaques DoS.

Parmi ces attaques, nous trouvons les attaques Syn-Flooding qui est la plus énervante qui soit, consiste à saturer le réseau ou le système en envoyant une multitude de paquets TCP avec le flag SYN armé, cela aura pour but de créer une multitude de connexions demandant un grand nombre de ressources système. La plupart des attaques par SYN-flood sont bien détectées par différents pare-feus, avec l'APF-firewall limitant les demandes d'établissement de connexion TCP acceptées à une par seconde et d'autre pare-feus.

2. Architecture du système :

La disponibilité de l'accès à une application ou un site web et aux données est un aspect critique des systèmes d'information d'aujourd'hui. Surtout pour le cloud computing qui offre des services à la demande par exemple e-commerce, de diffusion de vidéos, de récupération des données etc... . S'ils ne veulent pas perdre de clients, les fournisseurs doivent faire en sorte que leurs services soient accessibles en permanence et avec un niveau de qualité constant. Cela les oblige souvent à offrir des solutions de cloud sécurisées contre les différentes attaques qui menacent la confidentialité, la disponibilité et l'intégrité des sources de données et des services.

Pour cela, nous proposons dans notre travail une manière de protéger les services du cloud contre les attaques DoS qui causent généralement l'indisponibilité des services.

Notre solution repose sur l'architecture multi serveurs et la technique de répartition de charge utilisée en informatique pour distribuer un travail entre plusieurs serveurs. Cette dernière permet d'assurer l'extensibilité et la haute disponibilité d'applications et des sites web.

La répartition de charge interpose entre les utilisateurs de la ressource et le cluster un dispositif dénommé "répartiteur de charge" qui est capable de diriger l'utilisateur vers la ressource la moins occupée.

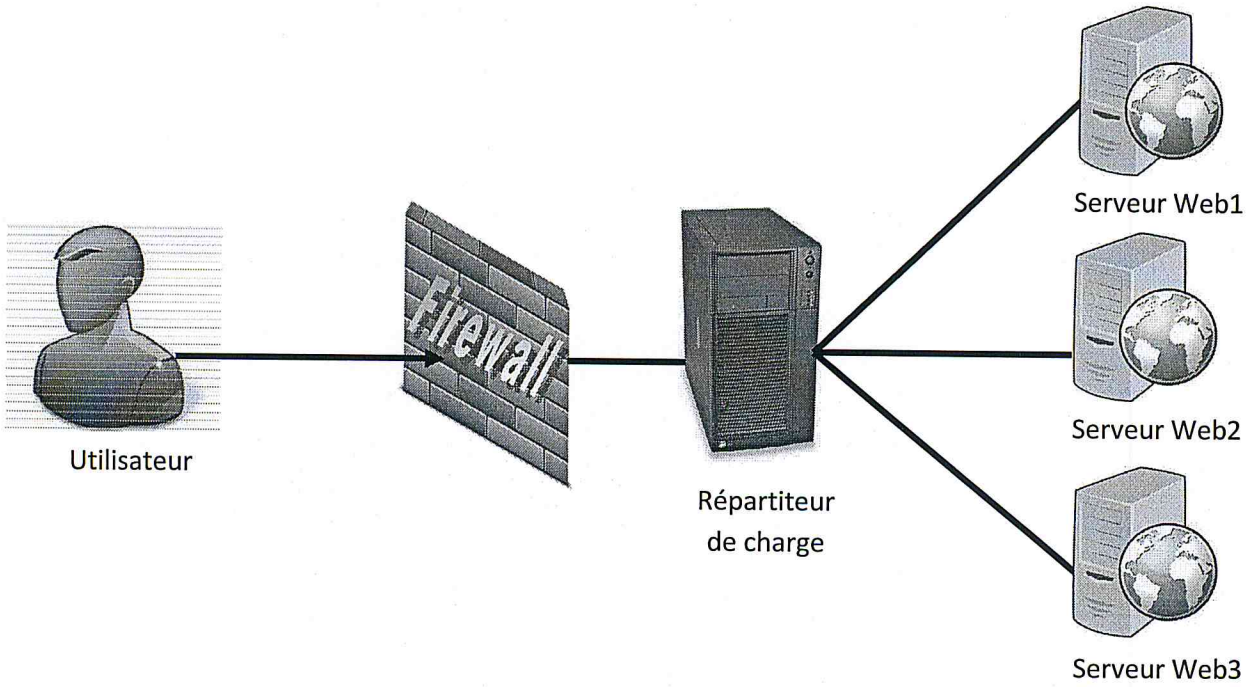


Figure 1: Architecture répartition des charges.

3. La modélisation :

Modéliser un système avant sa réalisation permet de mieux comprendre le fonctionnement du système. C'est également un bon moyen de maîtriser sa complexité et d'assurer sa cohérence.

Et pour la modélisation de notre système, on utilise la notion UML qui consiste un langage de modélisation et non pas une méthode objet.

3.1. Présentation du langage UML :

UML (Unified Modeling Language) est un langage de modélisation objet officiellement approuvé en 1997 par l'OMG (Object Management Group). UML "unifie" des méthodes de conception logicielle orientées objet - telles que Booch, OMT et OOSE - qui coexistaient jusque-là sans beaucoup de compatibilité entre elles. UML les rassemble non pas en en

proposant une synthèse, mais en créant un "langage de modélisation", c'est-à-dire une notation unique pour faciliter la conception de programmes. [58]

UML défini 9 diagrammes pour la représentation des systèmes :

- Diagrammes de cas d'utilisation.
- Diagrammes de séquence.
- Diagrammes de classe.
- Diagrammes d'activité.
- Diagrammes de composants.
- Diagrammes d'objets.
- Diagrammes d'interaction.
- Diagrammes d'états-transitions.
- Diagramme de collaboration.

3.2. Le modèle des cas d'utilisation :

Ces diagrammes déterminent les principales fonctions de notre système :

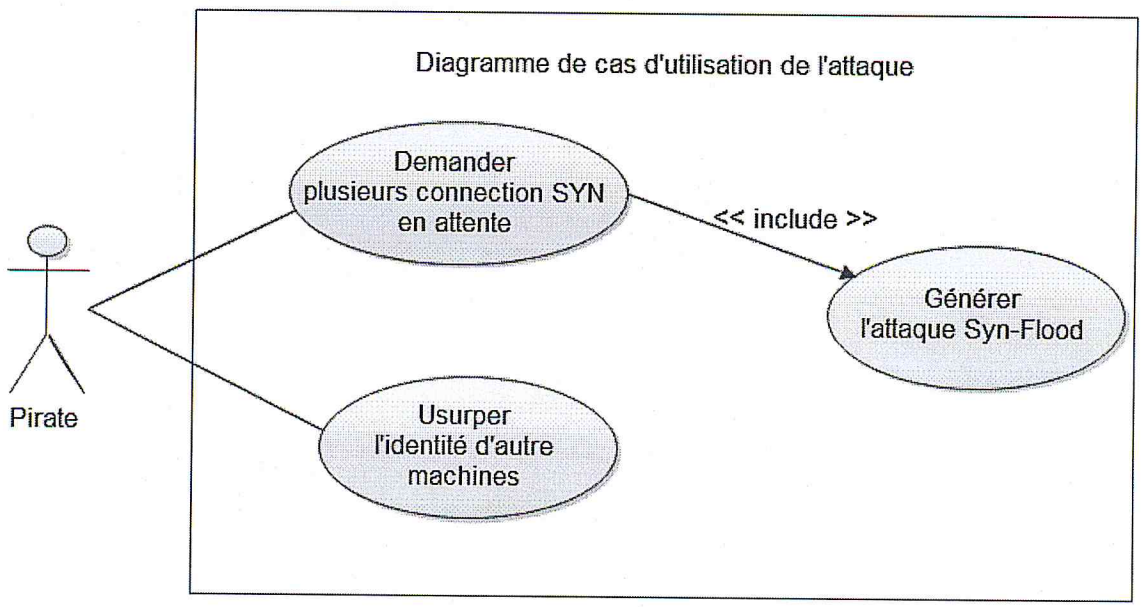


Figure 2: Diagramme de cas d'utilisation de l'attaque.

Acteur	Cas d'utilisation	Description
Pirate	La demande de plusieurs connections SYN	Le pirate génère l'attaque DoS de type Syn flooding et il usurpe une adresse IP d'un machine existantes dans notre réseau après il envoie plusieurs demandes de connexion aux serveurs afin de d'inonder les files d'attente de ces derniers afin de causer l'indisponibilité des serveurs

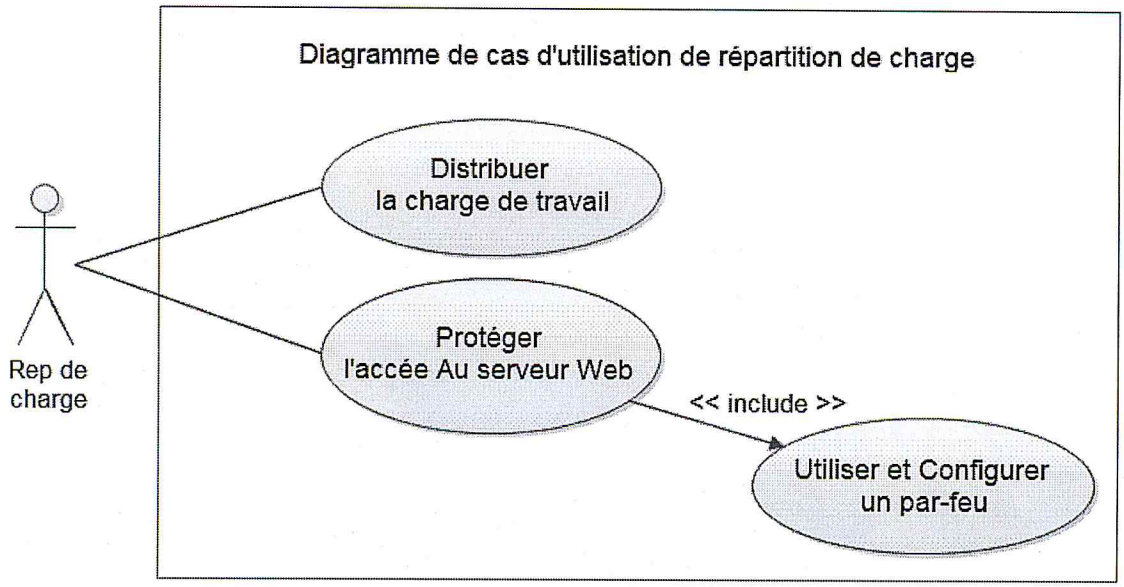


Figure 3: Diagramme de cas d'utilisation de répartition de charge.

Acteur	Cas d'utilisation	Description
Rep .de charge	Distribuer la charge du travail	La fonctionnalité du répartiteur de charge dans notre système est de distribuer la charge entre les serveurs existants dans notre réseau
	Protéger l'accès au serveur	Grâce au parfeu géré par le répartiteur, l'accès des utilisateurs sera contrôlé et

		filtré

3.3. Diagramme de séquence :

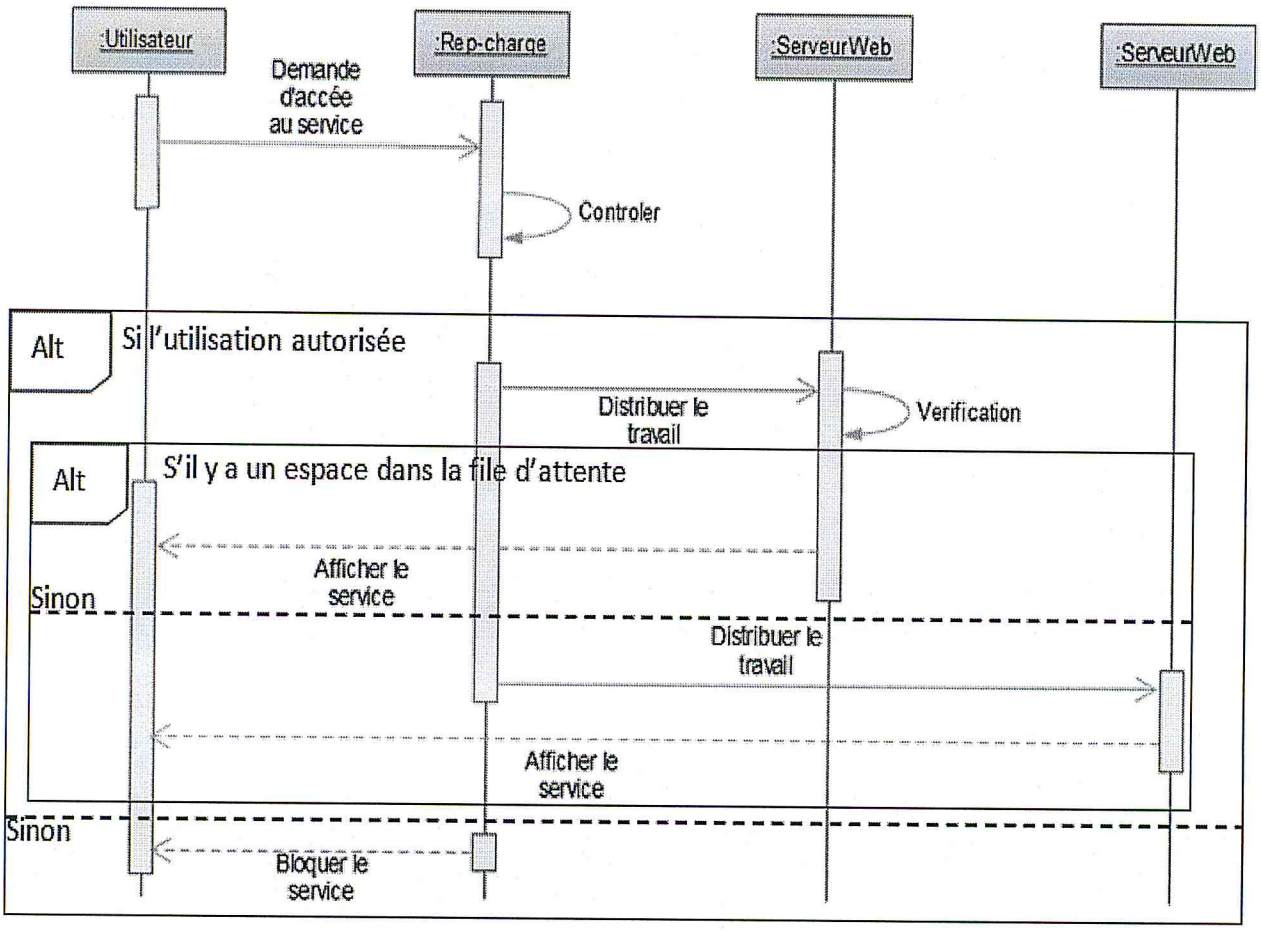


Figure 3: Diagramme de séquence l'accès à un service.

La description :

Quand l'utilisateur veut accéder à un service, il envoie une demande au répartiteur de charge qu'il va contrôler grâce l'utilisation d'un pare-feu l'autorisation d'accès pour cette demande après il envoie la demande au serveur web, si il existe un espace un espace dans leur file d'attente il accepte la demande de connexion et il affichera le service demandé si non il renvoie cette demande à un autre serveur

Si l'accès n'est pas autorisé au début le pare-feu va bloquer l'utilisateur.

3.4. Le diagramme de classe :

Le diagramme de classes est généralement considéré comme le plus important, dans un développement orienté objet. Il représente l'architecture conceptuelle du système : il décrit les classes que le système utilise, ainsi que leurs liens, que ceux-ci représentent un emboîtage conceptuel (héritage) ou une relation organique (agrégation, composition).

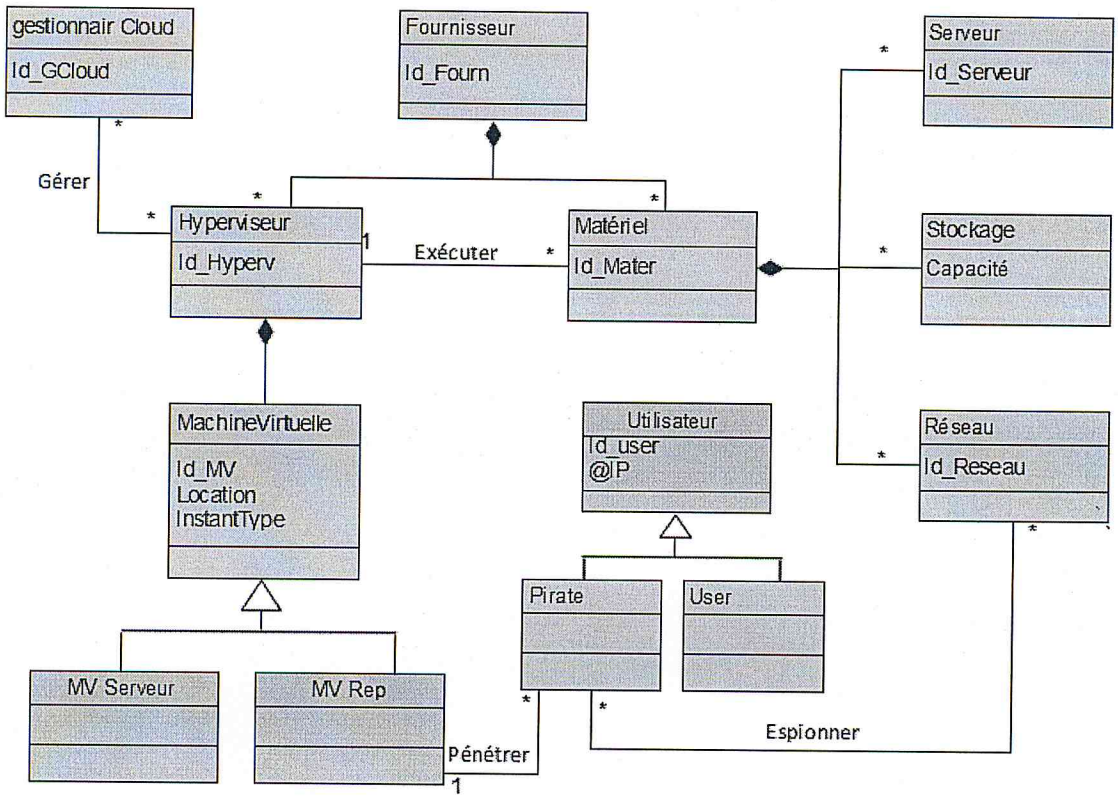


Figure 4:Diagramme de classe attaques DoS dans un réseau virtuel « Cloud ».

Entité	Attribut
Gestionnaire Cloud	Id_Gcloud
Fournisseur	Id_Fourn
Hyperviseur	Id_Hyperv
Matériel	Id_Mater
Machine Virtuelle	Id_VM Location

	InstantType @IP
Serveur	Id_Serveur
Stockage	Id_Stockage
Réseau	Id_Réseau
Utilisateur	Id_utilisateur @IP
MV ServeurWeb	ServerWeb_Apache
MV Répartiteur	ServerWeb_Nginx
Pirate	
User	

4. Conclusion :

La modélisation est une phase importante dans le développement d'un système car elle permet de créer une représentation simplifiée de notre problème: le modèle. Grâce à ce modèle il est possible de représenter simplement nos besoins en passant par l''analyse et la conception. Dans notre cas, nous avons utilisé les diagrammes d'UML qui fournissent un moyen astucieux permettant de représenter diverses projections d'une même représentation grâce aux ces différentes vues.

1. Introduction :

Dans notre travail, nous avons vu les différentes attaques par déni de service qui courent un risque permanent pour le Cloud Computing. Notre application est composé d'un hyperviseur qu'il est fournit des machines virtuelles qui les a mis dans un réseau locale, nous interessons à protéger une machine, contre l' accès non autorisé à partir d'un système d'expoitation invité. Nous avons besoin d'appliqué un pare-feu a une machine pour le protéger contre les pénètres d'une autre machine attaquante.

2. Les environnements logiciels :

Notre implémentation consiste à mettre en place un cloud qui se repose sur un cluster basé sur linux et sur d'autres outils libres.

2.1. L'hyperviseur Vmware workstation 7.0 pour crée les machines virtuelles :

VMware Workstation est plébiscité pour sa capacité à prendre en charge de nombreux systèmes d'exploitation, son environnement utilisateur complet, ses fonctionnalités multiples et ses performances élevées. Pour les spécialistes techniques, c'est un outil très utile qui valorise les applications conçues par des ingénieurs pour des ingénieurs.

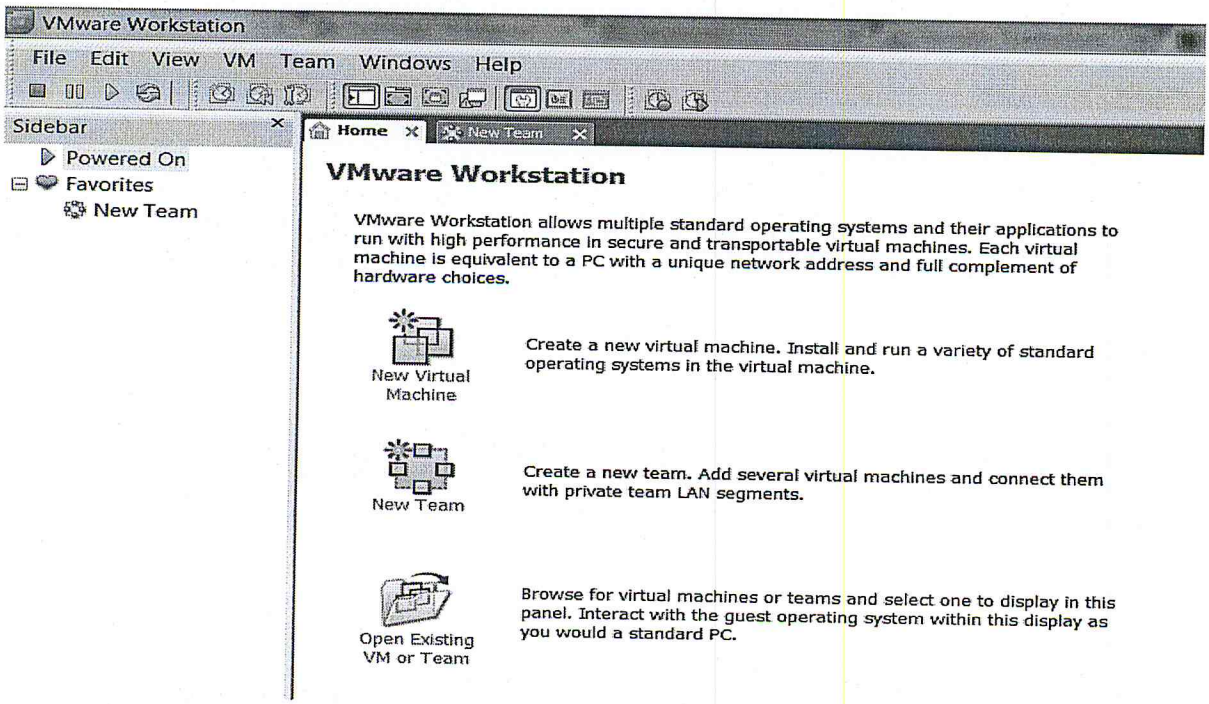


Figure 26 : l'interface graphique d'hyperviseur Vmware Workstation

Parmi les nouvelles fonctionnalités de VMware Workstation 9:

- **Prise en charge de Windows 8** – L'installation facile simplifie la création de machines virtuelles pour Windows 8 pouvant tourner simultanément sur divers systèmes d'exploitation existants. Le mode Unity fonctionne intelligemment avec les applications Windows 8, et la prise en charge du tactile en mode multi-touch assure une expérience Windows 8 authentique.
- **Des machines virtuelles plus puissantes** – Les applications les plus gourmandes tournent simplement et efficacement grâce à une meilleure vitesse de démarrage, à la prise en charge de l'USB 3.0 pour les machines virtuelles Windows 8, la compatibilité avec Intel™ Ivy Bridge, des extensions de virtualisation plus puissantes, des compteurs de performances de virtualisation, la prise en charge de l'OpenGL 2.1 sur Linux et des performances graphiques améliorées pour la 3D.
- **Mobilité accrue** – La nouvelle interface Web permet d'accéder à des machines virtuelles tournant sur Workstation ou sur VMware vSphere® à partir de tablettes, de téléphones portables ou d'ordinateurs de bureau. Cette interface Web aux performances élevées livre une expérience de poste de travail équivalente à celle des systèmes natifs et ne nécessite pas l'installation de la technologie flash, ni l'intégration de plug-ins à un navigateur.
- **Machines virtuelles sécurisées** – Les administrateurs et formateurs informatiques peuvent créer des machines virtuelles et les configurer afin d'empêcher leurs employés ou leurs étudiants de glisser-déplacer des fichiers entre des bureaux virtuels et physiques, de connecter des appareils ou de modifier les paramètres des machines virtuelles. Une fois les restrictions paramétrées, les machines virtuelles peuvent être cryptées et distribuées pour tourner sur des PC sur Mac, Windows ou Linux à l'aide de VMware Fusion 5 Professional, Workstation 9 ou VMware Player 5.

2.2. Le système d'exploitation Linux Ubuntu Server 12.04 :

Est un système d'exploitation libre commandité par la société Canonical et une marque déposée par cette même société.

Bien que peu connue du grand public, une version serveur existe. Ubuntu Server permet une installation rapide de LAMP sur toute machine basée sur l'architecture x86, AMD64 ou UltraSPARC T1. La principale différence entre Ubuntu Server et Ubuntu ou Kubuntu est le choix des paquets installés par défaut. Le nombre réduit de programmes installés favorise la sécurité du serveur et réduit la charge et les occupations mémoire et disque de celui-ci. L'installation et la

gestion de ce serveur se font en mode texte (ligne de commande). Malgré tout, tous les logiciels se trouvant dans les versions graphiques d'Ubuntu sont disponibles.

2.3. Le pare-feu APF :

Le pare-feu APF (advanced policy firewall) est un pare-feu basé sur **iptables** (netfilter) conçu autour des besoins essentiels des serveurs Linux d'aujourd'hui. La configuration est conçue pour être très intuitive et facile à suivre. La gestion au jour le jour est effectué à partir de la ligne de commande avec le «APF», qui comprend des informations détaillées sur l'utilisation de toutes les caractéristiques.

Le côté technique d'APF est tel qu'elle utilise les dernières fonctionnalités stables de l'iptables (netfilter) visant à fournir un pare-feu très robuste et puissant. Le filtrage est effectué par l'APF en trois volets:

- Les règles statiques basées des politiques statiques (ne pas confondre avec un pare-feu "statique").
- Une politiques stateful pour les connexions.
- Une politique de santé.

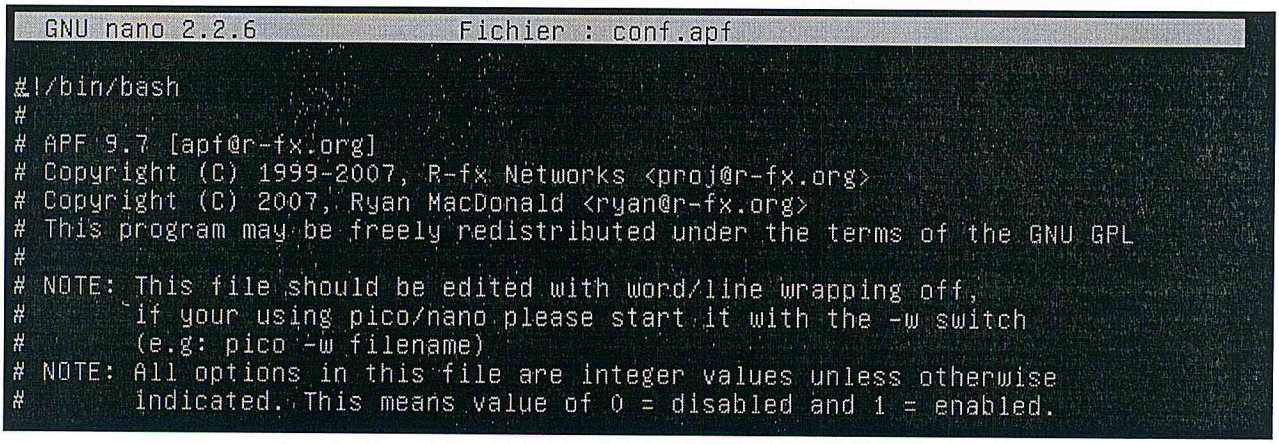


Figure 27 : Firewall APF

4. Préparation de l'infrastructure :

Pour mettre en place l'architecture ci-dessus, nous aurons besoins de quatre serveurs, tous ces serveurs seront équipés de système d'exploitation GNU/Linux, spécifiquement ubuntu Server 12.04.2 LTS.

Après l'installation des systèmes d'exploitation nous avons beseion d'utilisé des serveurs web NginX 1.2.8 et Apache 2.2.

4.1. Le répartiteur de charge :

Un répartiteur de charges est basé sur NginX qui permet de distribuer la charge sur les serveurs de notre réseaux afin d'éviter le blocage des services web en cas d'attaque DoS, il travaille sous le principe suivant :

Soient des Serveurs S1, S2, S3

Sj avec la même priorité,

Soient un Service V,

Soit une D,

Demande de Service D,

T0 temps maximum de la réponse,

Pour chaque Sj

Si Client demande V Alors Envoyer D au Sj

Si T réponse < T0 Alors Sj disponible

D réalisée

Sinon

Renvoyer D au Sj+1

Nous avons installé NginX 1.2.8 sur le répartiteur de charge souvent utilisé pour le reverse proxying, le proxy inverse est un type de serveur, habituellement placé en frontal de serveurs

web, Contrairement au serveur proxy qui permet à un utilisateur d'accéder au réseau Internet, il permet à un utilisateur d'Internet d'accéder à des serveurs internes.

Nous avons installé ce serveur avec la commande suivante :

```
root@ubuntu:/media/dvd/packages# bash ghaim.sh install lb-node_
```

4.2. Les serveurs web :

Nous avons installé Apache 2.2 sur les trois serveurs, Apache est le serveur web le plus répandu sur Internet permettant à des clients d'accéder à des pages web, c'est-à-dire en réalité des fichiers au format HTML à partir d'un navigateur (aussi appelé browser) installé sur leur ordinateur distant.

Nous avons installé ce serveur avec la commande suivante :

```
root@ubuntu:/media/dvd/packages# bash ghaim.sh install web-node_
```

5. Configuration :

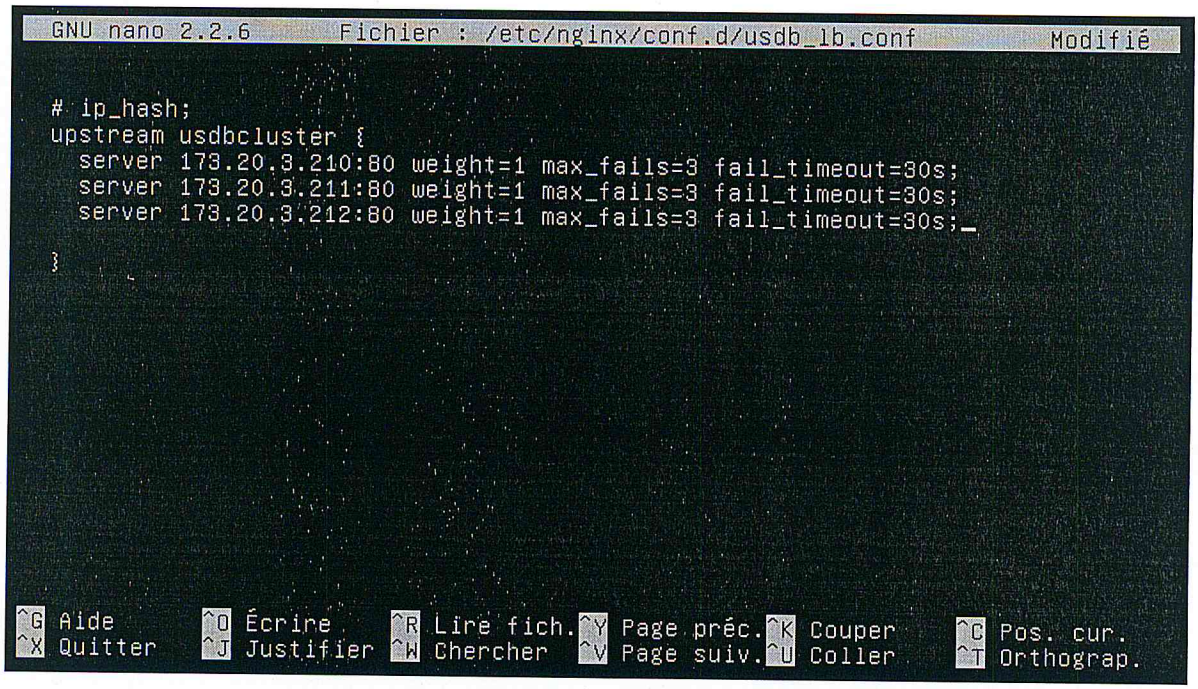
La configuration est basée sur des commandes Linux.

5.1. Les répartiteurs de charge :

Le fichier de configuration de NginX est avec la commande :

```
root@ubuntu:~# nano /etc/nginx/conf.d/*.conf_
```

On doit ajouter les IP des serveurs web ainsi que leurs poids selons une syntaxe bien précise sur ce fichier de configuration :

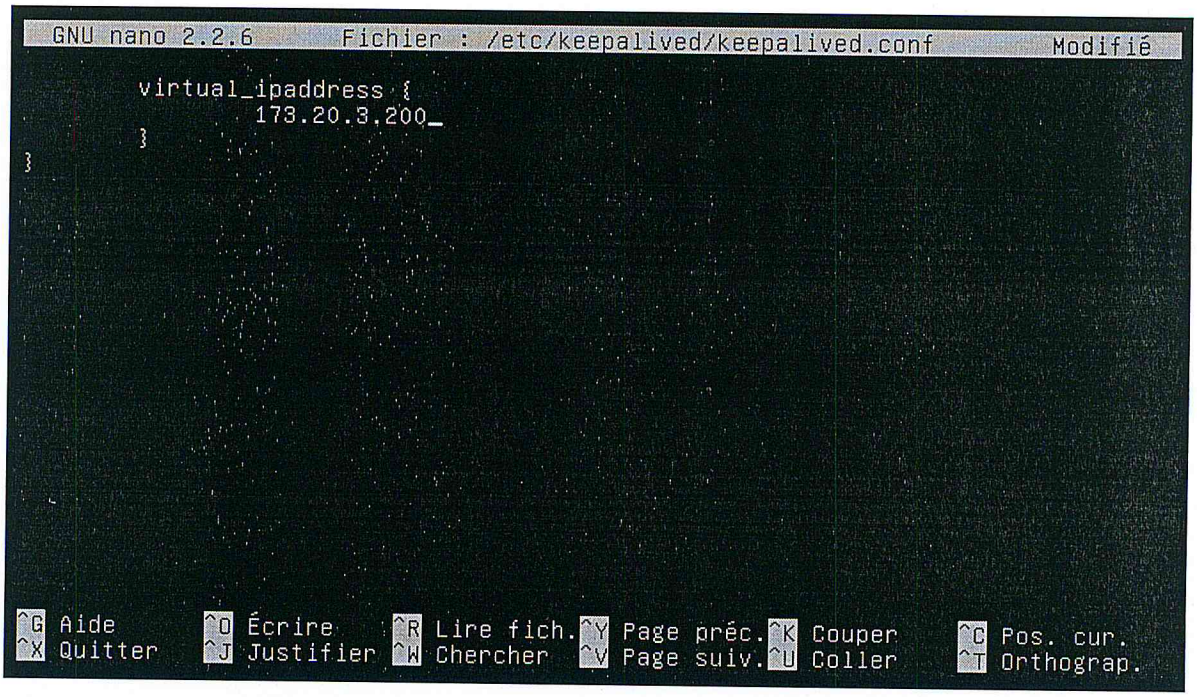


Ce fichiers est de configuration de serveur NginX, il contient les paramètres de répartiteur de charge, la première clause est une déclaration de UpStream (les Serveur web) où chaque ligne représente un serveur web, chaque serveur a une adresse IP, poids (poids plus élevé est le plus charge à rediriger vers ce serveur), si le répartiteur de charge à rediriger 3 requêtes respectivement (max_fails) vers ce serveurs sans répondre il va lui retirer automatiquement pendants 30s (fail_timeout).

Il faut aussi configurer le paquet "keepalived" avec la commande :

```
root@ubuntu:~# nano /etc/keepalived/keepalived.conf_
```

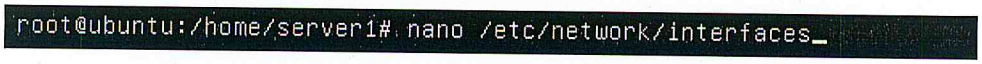
Pour modifier l'IP virtuel :



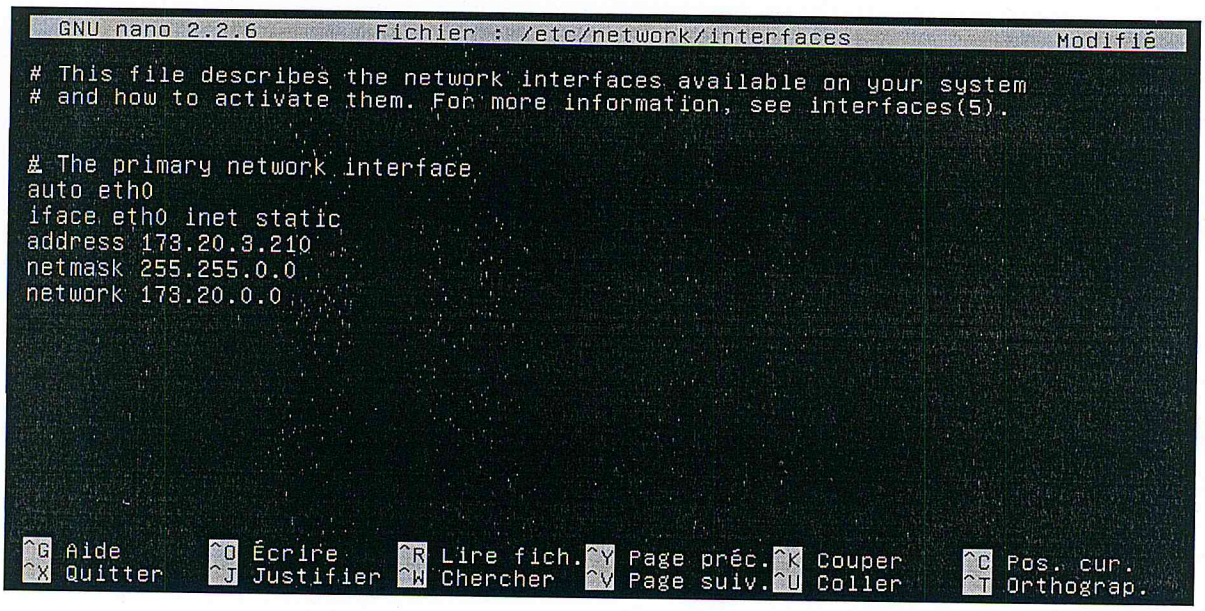
Virtual_ipaddress : Est l'adresse IP qui sera accessible à tous les clients. Les clients seulement accéder à cette adresse IP.

5.2. Les Serveurs Web :

Pour la configuration des adresses IP par la commande suivant :



Et pour le programmé sur le fichier suivant :



Il doit mettre l'adresse IP (address) de serveur et leur adresse masque (netmask) et l'adresse de réseau (network), Sur chaque serveur.

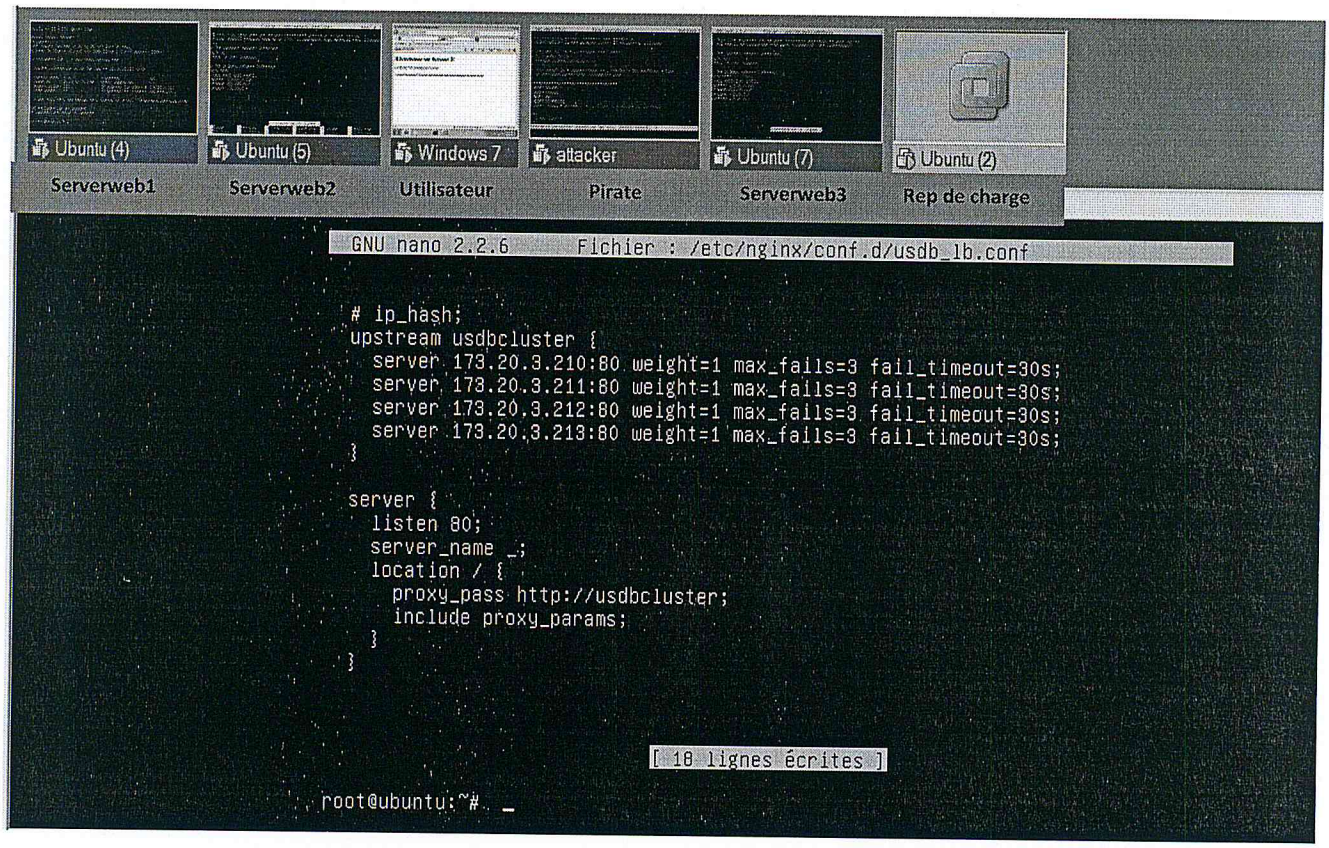
L'affichage de page web par défeaut d'un Serveurs Web existe sur le fichier index.html qui est programmé par le longage HTML, il est par la commande suivante :

```
root@ubuntu:/home/server1# nano /var/www/index.html_
```

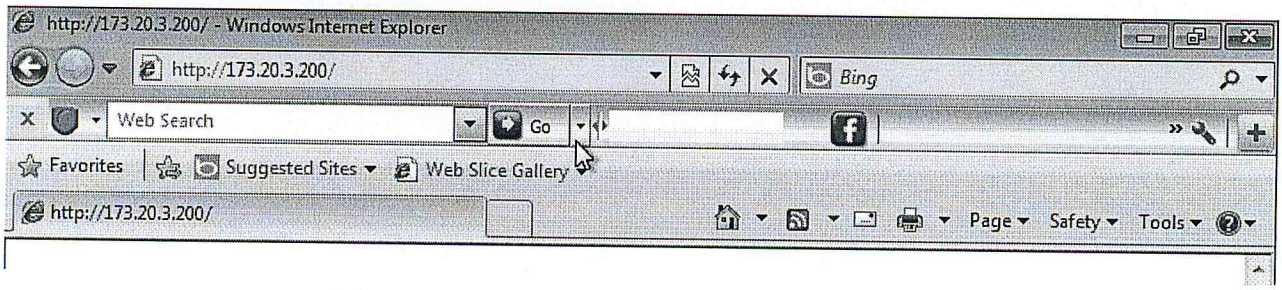
Le contenu de fichier :

```
  GNU nano 2.2.6          Fichier : /var/www/index.html          Modifié

 <html><body><h1>Il fonctionne sur Serveur 1!</h1>
<p>C'est la page Web par defaut pour ce serveur.</p>
<p>Ce logiciel de serveur Web est en cours d'execution
mais aucun contenu n'a ete ajoute encore.</p>
</body></html>

Sauver l'espace modifié (RÉPONDRE « Non » EFFACERA LES CHANGEMENTS) ?
```

6. Tests :

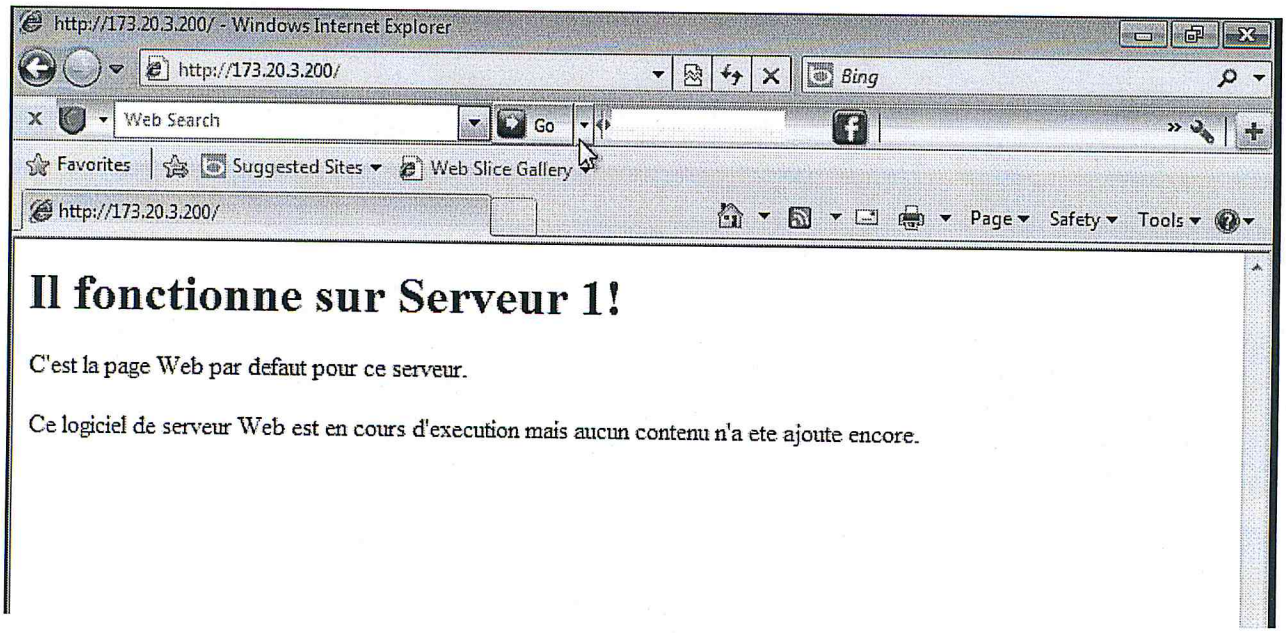


Notre système contient des serveurs et des machines virtuelles, lors de la demande d'un utilisateur un accée à un service

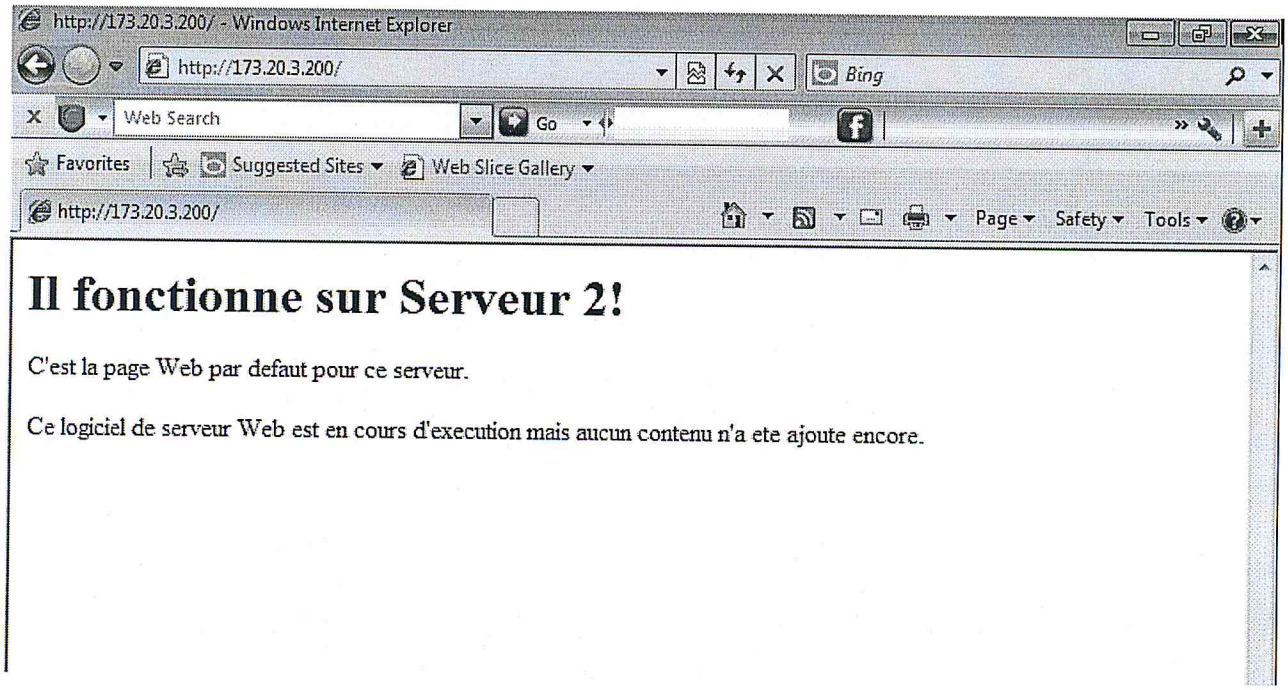


Pour éviter l'inondation de la demande de connection SYN une attaque SYNFlood sur le serveur Le répartiteur de charge va distribuer la demande au Serveur web,

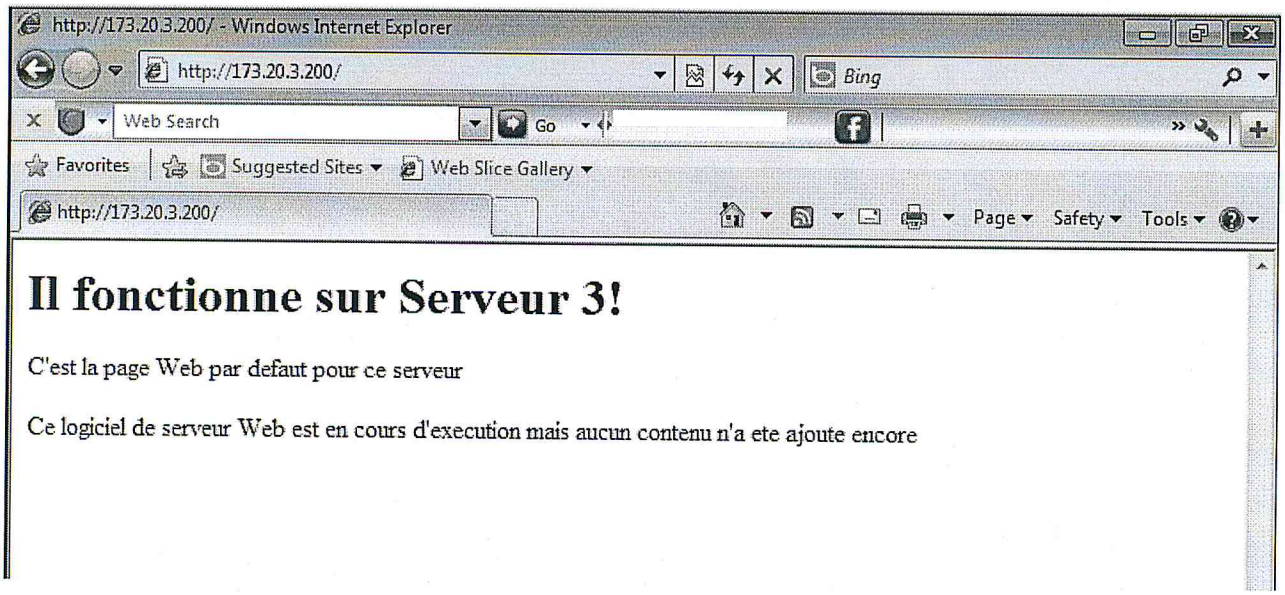
Il commence par le premier serveur sachant qu'il n ya pas la notion de priorité entre les serveurs :



Si le premier serveur est en charge le répartiteur va redistribuer au deuxième,

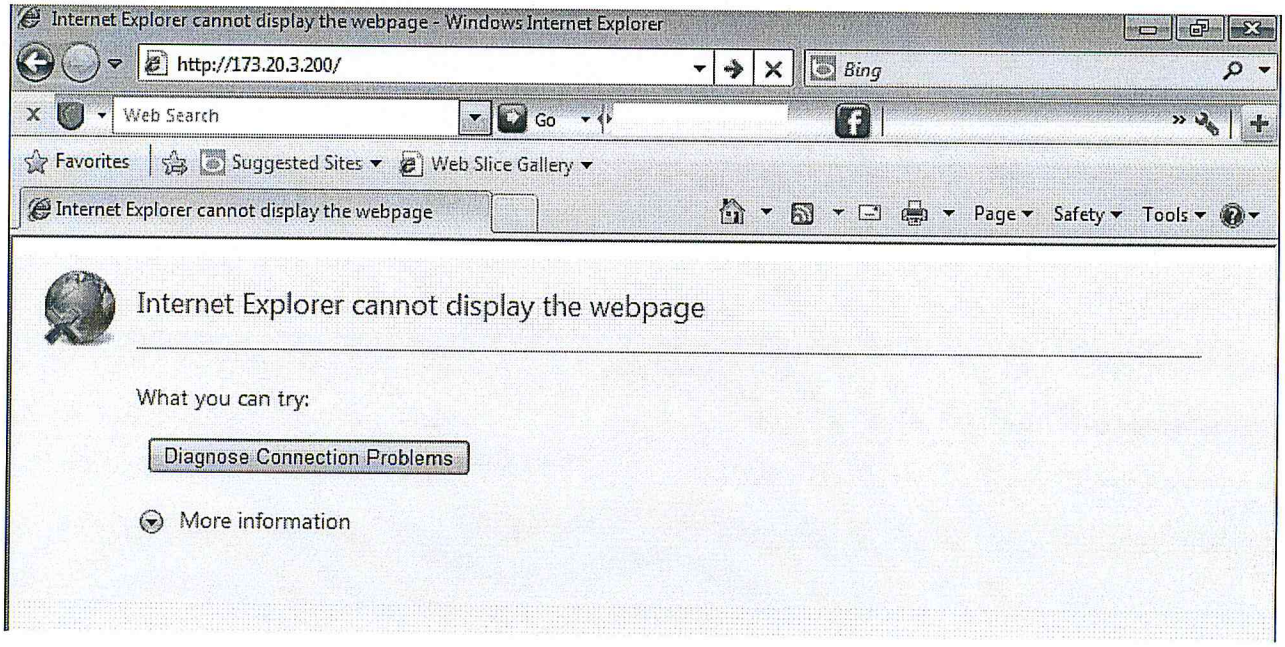


Aussi si le deuxième est en charge le répartiteur va transformer le travail au dernier.



Et pare ce que le serveur n'a pas lui ajouter aucun contenu il n'affiche que la page par défaut.

Si l'utilisateur est non autorisé il ne peut pas accéder aux services.



7. Conclusion :

Dans ce chapitre, nous avons détailllé pratiquement notre architecture de préparation, configuration et les tests en assurant la haute disponibilité des services à la demande aux utilisateurs autorisé grâce à notre mode de sécurité.

Conclusion Général

Le Cloud Computing est une technologie en plein essor permet aux entreprises de disposer d'infrastructures et de progiciels directement en ligne sur Internet. On a distingué les différents types de Cloud possibles avec l'IAAS pour les infrastructures techniques, le PAAS pour les infrastructures habillées avec des outils de middleware comme les bases de données par exemple et le SAAS pour les services logiciels. Ces trois types peuvent se déployer sous quatre formes de topologies différentes : le Cloud public pour du déporté en ligne, le Cloud privé pour l'utilisation des concepts du Cloud en interne à l'organisation, le Cloud hybride pour l'utilisation commune du public et du privé et enfin le mode communautaire pour des entreprises géographiquement proches ou à intérêts communs.

Et le domaine de sécurité de cette technologie reste un domaine très vaste et indispensable, pour cela, il faut donner une grande importance à ce domaine et le prendre en considération parce que, de nos jours, presque toutes des entreprises utilisent le Cloud Computing qui contient des failles que la majorité vient à cause du mauvaise développement.

Les attaques par déni de service parmis les attaques qui pénétrent le Cloud, ils ont existent depuis longtemps et se sont développées au fur et à mesure de l'évolution des systèmes informatiques. Etant simples d'accés, elles sont trés utilisées dans de nombreuses situations, et deviennent meme parfois politique.

Ces attaques sont trés modulables et bien que la détection fait d'énormes progrés, elles restent toujours trés compliques à mettre en place de manière efficace. Il ne suffit pas de multiplier les outils de préventions et d'enrichir ses connaissances. Il faut surtout etre réactif et se préparer à toutes les éventualités. Il faut aussi voir l'aspect financier de ces attaques et adapter le budget de protections aux risques encourus. Mais le risque zéro ne sera jamais atteint et plus les technologies évolues, plus les pirates auront accés à des ressources importantes. Les attaques seront alors trés compliquées, voire impossible à contrer avec les méthodes actuelles. La course contre les pirates ne s'arrétera jamais.

Références

[1] Le Cloud Computing : Réelle révolution ou simple évolution? Bureau d'entreprise technologique

[2] www.figer.com

[3] behind-cloud-computing.com, janvier 2011

[4] Cloud Computing : la stratégie de Microsoft, Bernard Ourghanlian, Chief Technology & Security Officer, Microsoft France, 2009

[5] Le cloud privé et ses avantages métiers : des coûts réduits et une réactivité accrue, EMC Corporation, 2010

[6] www.renaudvenet.com, janvier 2011

[7] Mag.welovesaas.com, févr. 2012, CLÉMENT VOUILLON

[8] social.technet.microsoft.com

[9] Une plateforme de type cloud pour un centre d'examen en ligne basé sur la plateforme Moodle A BELKHIRI, A FERHATI 2012

[10] Blogs.technet.com

[11] onlinehelp.hostbasket.com, novembre 2011

[12] www.itresearch.fr, novembre 2012

[13] bagdatli.fr, février 2013

[14] État de l'art des solutions libres de virtualisation pour une petite entreprise Lucas Bonnet

[15] www.microsoft.com

[16] www.le-libriste.fr, mai 2009

[17] Déploiement d'une solution de virtualisation au sein d'une multinationale, RAYNAUD Philippe, mars 2011

[18] Réduction des coûts d'investissement avec la mise en place d'un environnement de virtualisation en production à la DTAI, Cheikh Saadbouh Tall, 2006

[19] Virtualisation de réseau et supervision BUCHER Aurélie,FRITZ Jean-Nicolas, LAMBERT Florian, LAMBERT Gaël, Projet tutoré 2008-2009

[20] www.nrconsulting.fr/virtualisation.html

[21] www.faronics.com, mars 2012, Dmitry Shesterin

[22] www.equasys.fr/vpn.php

[23] La virtualisation, François Santy, Projet de Recherche et Communication Scientifique Année académique 2009 – 2010

[24] www.ntsysv.com, novembre 2008

[25] www.neoflow.fr, novembre 2012

[26] Compte rendu de la conférence du 20 janvier 2009 : Virtualisation, cloud computing et SaaS. le Club ESSEC Business & Technologie et les Groupes professionnels Informatique et Télécom de l'école des Mines, Grenoble Ecole de Management et Reims management school, les clubs professionnels ESSEC PME-PMI et ESSEC Marketing

[27] www.deocia.com

[28] Livre blanc La sécurité et la virtualisation, polytech lyon, David GELIBER, Farid SMILI, Jérôme DEROCK, Loïc RATSIHORIMANANA, Mickaël DREYER, Thomas GERVAISE, mai 2012

[29] jerome.derock.free.fr

[30] Approche logique pour l'analyse de traces d'exécutions, Mémoire, Québec, Canada, Rimeh Zribi, 2013

[31] Master 2 Professionnel STIC-Informatique – Module ARS

[32] www.memoireonline.com

[33] www.numilog.fr

[34] www.syntec-numerique.fr

[35] www.commentcamarche.net

[36] www.hackersrepublic.org

[37] Sécurité des réseaux Les attaques des réseaux ; A. Guermouche

Références

[38] Type d'attaques, Stéphane Gill, 2003

[39] www.futura-sciences.com

[40] www.howstuffworks.com

[41] www.securiteinfo.com

[42] www.securite-informatique.gouv.fr

[43] www.techno-science.net

[44] thomas.vivet.free.fr

[45] www.dicofr.com

[46] www.authsecu.com, novembre 2006, par Sébastien FONTAINE

[47] Ecole Nationale Supérieure des Télécommunications, Institut de la Francophonie pour l'Informatique, RAPPORT DE STAGE DE FIN D'ETUDES, Etudiant : DOAN DUY Thieu Hoa, IFI, Responsables Ahmed SERHROUCHNI, Paris, janvier - juillet 2004

[48] La protection des réseaux contre les attaques DoS, Amarir Hakim Danes Adrien Doé Sidney, Mai 2009

[49] La protection des réseaux contre les attaques DOS, Dany Fernandes et Papa Amadou Sarr, Mai 2010

[50] www.anti-cybercriminalite.fr

[51] Protection contre les attaques de déni de service dans les réseaux IP, Osman SALEM, HOTTE Marion, LUTUN Quentin-Edouard, ASCOET Thomas

[52] Déni de service distribué (DDoS), NICOLAS FORTIER, FRANCOIS-PHILIPPE IL GRANDE, mars 2003

[53] www.commentcamarche.net, Avril 2013

[54] www.k-tux.com, octobre 2010

[55] wiki.backtrack-fr.net, décembre 2010

[56] www.awt.be,janvier 2005

Liste des abréviations

ASP	: Application Service Provider
IBM on demande	: International Business Machines
IaaS	: Infrastructure as a service
PaaS	: Platform as a Service
SaaS	: Software as a Service
TCP/IP	: Transmission Control Protocol/Internet Protocol
Amazone EC2	: Amazone ElasticCompute
AmazoneS3	: Amazon Simple Storage Service
OS	: operating system
CRM	: Customer Relationship Management
VM/CMS	: Virtual machine/Classic Model Cars
IBM	: nternational Business Machines
HP	: Hewlett-Packard
IA64	: Intel Architecture 64 bits
MV	: Machine virtuel
MAC	: media access control
SE	: Système d'exploitation
Intel VT	: la technologie de virtualisation Intel
AMD-V	: Advanced Micro Dynamics-virtalisation
CPU	: Central Processing Unit
VLAN	: Virtuel LAN
IPX	: InternetworkPacket Exchange
SATA	: standard Serial ATA
SCSI	: Small Computer System Interface
LVM	: logical volume management
PPC	: Pay-per-click
QEMU	: Quick EMUlator
ftp	: File Transfer Protocol
NFS	: Need For Speed
MTU	: maximum transmission unit